

Окончательный отчет по итогам работы над Фазой 2А ускоренного процесса формирования политики по Временной спецификации для регистрационных данных в gTLD

3 сентября 2021 года

Статус этого документа

Это итоговый отчет с рекомендациями группы по ускоренному процессу формирования политики GNSO (EPDP) по Временной спецификации для регистрационных данных в gTLD, подготовленный в рамках Фазы 2А для передачи Совету GNSO.

Преамбула

Целью этого итогового отчета является документирование следующих аспектов деятельности группы по EPDP: (i) результаты обсуждения вопросов устава группы, (ii) полученные комментарии относительно первоначального отчета по итогам работы над Фазой EPDP и их последующий анализ группой по EPDP, (iii) рекомендации по политике с указанием соответствующих уровней консенсуса и (iv) указания по выполнению рекомендаций, представленные на рассмотрение Совета GNSO.

Содержание

1	ОСНОВНЫЕ ПОЛОЖЕНИЯ	3
1.1	Для справки	4
1.2	Первоначальный отчет	5
1.3	Ответы и рекомендации	5
1.4	Выводы и дальнейшие действия	12
1.5	Другие важные разделы этого отчета	12
2	ПОДХОД ГРУППЫ ПО ЕРДР	13
2.1	Методология работы	13
2.2	Справочные материалы и подход	13
2.3	Юридический комитет	13
2.4	Вопросы Совета	14
3	ОТВЕТЫ ГРУППЫ ПО ЕРДР НА ВОПРОСЫ СОВЕТА И ЕЕ РЕКОМЕНДАЦИИ	15
•	3.1 Проведение различия между физическими и юридическими лицами	16
•	Ответ группы по ЕРДР на вопрос I.	16
•	Ответ группы по ЕРДР на вопрос II.	19
•	3.2 Возможность индивидуальных контактов	27
•	Ответ группы по ЕРДР на вопрос I.	32
•	Ответ группы по ЕРДР на вопрос II.	32
4	ДАЛЬНЕЙШИЕ ДЕЙСТВИЯ	34
	ГЛОССАРИЙ	35
	ПРИЛОЖЕНИЕ А. ИСТОРИЧЕСКАЯ СПРАВКА	42
	ПРИЛОЖЕНИЕ В. ОБЩИЕ СВЕДЕНИЯ	43
	ПРИЛОЖЕНИЕ С. СОСТАВ ГРУППЫ ПО ЕРДР И УЧАСТИЕ В ЗАСЕДАНИЯХ	46
	ПРИЛОЖЕНИЕ D. ЗАЯВЛЕНИЯ МЕНЬШИНСТВА	50
	ПРИЛОЖЕНИЕ E. ВКЛАД СООБЩЕСТВА	94
	ПРИЛОЖЕНИЕ F. ЮРИДИЧЕСКИЕ РЕКОМЕНДАЦИИ BIRD & BIRD	95

Настоящий документ был переведен на несколько языков только для информационных целей. Оригинал и аутентичный текст документа (на английском языке) находится по адресу: <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2a-updated-final-report-03sep21-en.pdf>

1 Основные положения

1.1 Для справки

17 мая 2018 года Правление ICANN утвердило Временную спецификацию для регистрационных данных в доменах общего пользования верхнего уровня (gTLD), чтобы обеспечить возможность соблюдения сторонами, связанными договорными обязательствами, существующих контрактных требований ICANN при одновременном соблюдении Общих положений о защите данных (GDPR) Европейского Союза. Исходя из этого решения Правления, 19 июля 2018 года Совет GNSO инициировал PDP. PDP был проведен в две фазы: задача Фазы 1 заключалась в том, чтобы утвердить или не утвердить Временную спецификацию к 25 мая 2019 года; Фаза 2 предполагала, среди прочего, обсуждение модели стандартизированного доступа к закрытым регистрационным данным gTLD и их раскрытия (SSAD).

Совет GNSO утвердил итоговый отчет по Фазе 2 на заседании 24 сентября 2020 года; однако по просьбе некоторых участников группы по EPDP, Совет GNSO [предложил](#) группе по EPDP продолжить работу над двумя темами: 1) дифференциация регистрационных данных юридических и физических лиц и 2) возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов. Эти две темы были рассмотрены на Фазе 2А.

Говоря конкретно, группе по EPDP были даны следующие поручения:

- а) Что касается дифференциации юридических и физических лиц, ожидается, что группа по EPDP рассмотрит [результаты предпринятого корпорацией ICANN исследования](#) (выполненного по запросу группы по EPDP и одобренного Советом GNSO во время Фазы 1) наряду с [юридическими рекомендациями](#) компании Bird & Bird, а также предложениями по существу данного вопроса, поступившими в ходе [общественного обсуждения](#), и ответит на следующие вопросы:
 - i. Необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»);
 - ii. Необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие.
- б) Что касается возможности использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, ожидается, что группа по EPDP проанализирует [юридические](#)

[рекомендации](#) и рассмотрит конкретные предложения в отношении достаточных мер защиты, призванных устранить проблемы, отмеченные в докладной записке по юридическим вопросам. На группы, которые попросили выделить им дополнительное время на рассмотрение этой темы (ALAC GAC и SSAC), возлагается ответственность за выработку соответствующих конкретных предложений. В итоге предполагается получить ответы на следующие вопросы:

- i. Имеется ли возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, и если да, должно ли это стать требованием.
- ii. Если это осуществимо, но не является требованием, какие указания следует дать связанным договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты.

1.2 Первоначальный отчет

3 июня 2021 года группа по EPDP опубликовала свой [первоначальный отчет для общественного обсуждения](#). В первоначальном отчете излагались размышления группы до этого момента, и он должен был служить инструментом для выяснения мнения сообщества, особенно в тех областях, где сохранялись значительные разногласия. Хотя предварительные рекомендации были включены в первоначальный отчет, группа по EPDP попросила рассмотреть эти рекомендации в совокупности с рядом поставленных вопросов, чтобы способствовать доработке отчета.

После опубликования первоначального отчета группа по EPDP: (i) внимательно ознакомилась с комментариями, полученными во время общественного обсуждения первоначального отчета, (ii) продолжила анализ незавершенной работы вместе с группами сообщества, представленными в составе группы и (iii) продолжила обсуждение для подготовки итогового отчета, который будет рассмотрен Советом GNSO и, в случае утверждения, передан Правлению ICANN для принятия в качестве согласованной политики ICANN. В соответствии с требованиями Руководства для Рабочих групп GNSO председатель группы по EPDP провел опрос, чтобы оценить уровень консенсуса по каждой рекомендации, включенной в состав итогового отчета. Резюме:

1.3 Ответы и рекомендации

Заявление председателя

Хотя данный итоговый отчет и его рекомендации получили единодушную поддержку со стороны группы по EPDP 2А, важно отметить, что некоторые группы

сообщества сочли, что работа выполнена в недостаточном объеме или вопросы рассмотрены недостаточно подробно, в то время как другие группы сочли определенные рекомендации нецелесообразными или ненужными. Кроме того, на заключительном этапе нашей работы некоторые группы предпочли бы иметь возможность присвоить более детальные обозначения уровня консенсуса в отношении составных частей рекомендаций. В этом контексте всем читателям итогового отчета по EPDP 2A следует также ознакомиться с представленными каждой группой заявлениями меньшинства, которые прилагаются к итоговому отчету и входят в его состав, и исторической справкой о нашей работе.

Помимо достигнутого в отношении рекомендаций итогового отчета консенсуса есть ряд областей, в которых группы, принимавшие участие в Фазе 2A EPDP, не пришли к полному согласию, включая вопрос о том, должна ли дифференциация регистрационных данных юридических и физических лиц быть обязательной или факультативной, а также вопрос о том, уравнивается ли польза от публикации регистрационных данных юридических лиц риском непреднамеренного раскрытия персональных данных. Рекомендации, содержащиеся в итоговом отчете, практически не повлияли на эти расхождения во мнениях и точках зрения.

Настоящий итоговый отчет представляет собой компромисс, который является максимумом того, что могла достигнуть группа на данный момент в рамках выделенного нам времени и установленного круга задач, и его не следует рассматривать как результат, который полностью удовлетворил всех. Это подчеркивает важность заявлений меньшинства для понимания полного контекста рекомендаций итогового отчета.

Подробнее об этих обозначениях см. в разделе 3.6. [Руководства для Рабочих групп GNSO](#).

Полный текст рекомендаций и ответов см. в разделе 3.

Ответ на поручение Совета (a)(i).

Группа по EPDP дает следующий ответ на поручение Совета оценить необходимость изменения рекомендации по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»):

Группа по EPDP не достигла консенсуса по предлагаемым изменениям рекомендации № 17.1 по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»).

Предложение Совету GNSO

Группа по EPDP признает, что текущие и будущие законодательные изменения могут потребовать дополнительной работы над политикой в этой области, например, для разрешения потенциальных конфликтов с существующими требованиями политики и/или для рассмотрения вопроса о том, существует ли риск сегментации рынка, который необходимо устранить. В то же время, группа по EPDP признает, что до принятия законодательства, возможно, не удастся точно оценить его влияние. Группа по EPDP рекомендует Совету GNSO следить за этими событиями через отчеты о ситуации в законодательной/нормативной сфере, которые публикует корпорация ICANN.

Отмечая текущие обсуждения и ожидаемое принятие уточненной редакции Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем (NIS2), группа по EPDP настоятельно рекомендует Совету GNSO согласно существующим процедурам определить рамки возможной будущей работы в области политики после принятия NIS2, чтобы оценить, считается ли желательной и/или необходимой дальнейшая разработка политики.

Указания по дифференциации

Рекомендация № 1

Группа по EPDP рекомендует **ОБЯЗАТЕЛЬНО** создать поле или поля, чтобы способствовать дифференциации регистрационных данных юридических и физических лиц и/или определению наличия персональных данных в составе регистрационных данных. Корпорация ICANN **ДОЛЖНА** координировать свои действия с техническим сообществом, например с Рабочей группой по RDAP, для разработки всех необходимых стандартов, связанных с использованием этого поля или полей в EPP и RDDS.

Такое поле или поля **МОГУТ** использоваться сторонами, связанными договорными обязательствами, которые разграничивают регистрационные данные юридических и физических лиц и/или указывают, входят ли в состав регистрационных данных персональные данные или нет. Во избежание неопределенности поясняется, что стороны, связанные договорными обязательствами, **МОГУТ** использовать указанное поле (поля). Это означает, что, если сторона, связанная договорными обязательствами, принимает решение не использовать такое поле, оно может быть оставлено пустым или отсутствовать. Кроме того, стороны, связанные договорными обязательствами, **МОГУТ** включить это поле (поля) в ответ RDDS.

SSAD, в соответствии с рекомендациями по итогам Фазы 2 EPDP, ДОЛЖНА поддерживать такое поле или поля для содействия интеграции между SSAD и системами сторон, связанных договорными обязательствами. Это поле (поля) должно быть способно вместить следующие значения:

Правовой статус

- Разграничение по правовому статусу не проводилось (значение по умолчанию)
- Не указано — свидетельствует, что это не указано владельцем зарегистрированного имени и/или регистратором
- Владелец зарегистрированного имени является физическим лицом
- Владелец зарегистрированного имени является юридическим лицом

Персональные данные

- Наличие персональных данных не определялось (значение по умолчанию)
- Не указано — свидетельствует, что это не указано владельцем зарегистрированного имени и/или регистратором
- Регистрационные данные содержат персональную информацию
- Регистрационные данные НЕ содержат персональную информацию

Ответ на поручение Совета (a)(ii).

Рекомендация № 2

Группа по EPDP считает, что связанным договорными обязательствами сторонам, решившим проводить дифференциацию по типу лица, СЛЕДУЕТ выполнять приведенные ниже указания¹ и четко документировать все этапы обработки данных. Однако в задачи и обязанности группы по EPDP не входит принятие окончательного решения в отношении юридических рисков, поскольку такая ответственность в конечном итоге лежит на контролере (контролерах) данных.

GDPR защищает права физических лиц в сфере обработки их персональных данных. Действие GDPR не распространяется на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица. [Преамбула 14, GDPR] Это обычно позволяет раскрывать данные юридических лиц, поскольку они не входят в сферу действия GDPR; однако при обработке данных юридических лиц стороны, связанные договорными

¹ Обратите внимание, что представители корпорации ICANN предоставили группе по EPDP следующую информацию о том, как эти указания будут реализованы после их одобрения:
<https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html>.

обязательствами, должны принять меры предосторожности, чтобы избежать разглашения данных, позволяющих идентифицировать физическое лицо, в составе данных, обозначенных как данные юридического лица, поскольку это пример информации, которая *входит* в сферу действия GDPR. Подробнее об этом различии см. в [письме](#) Европейского совета по защите данных, начиная со стр. 4.

1. Владельцам доменов следует разрешить самостоятельно идентифицировать себя как физическое или юридическое лицо. Регистраторы должны предоставить владельцам доменов эту возможность самоидентификации в качестве физических или юридических лиц (i) в момент регистрации или без неоправданной задержки после регистрации² и (ii) в момент обновления владельцем домена контактной информации или без неоправданной задержки после обновления контактной информации.
2. Любой процесс дифференциации должен гарантировать вымарывание данных физических лиц из общедоступной RDDS за исключением случаев, когда субъект данных дал согласие на публикацию этих данных или они могут быть опубликованы на другом законном основании согласно GDPR в соответствии с подходом «защита данных по замыслу и по умолчанию», изложенным в статье 25 GDPR.
3. В рамках внедрения регистраторам следует рассмотреть возможность использования поля (полей), описанного в рекомендации № 1, в RDDS, SSAD или их собственных наборах данных, где будет указан тип соответствующего лица (физическое или юридическое), а в случае юридического лица также и тип соответствующих данных (персональные или не относящиеся к персональным). Такая маркировка могла бы содействовать рассмотрению запросов на раскрытие информации и выполнению требований по автоматизации SSAD и предоставлению данных юридических лиц, не относящихся к персональным, системами, отличными от SSAD (такими как WHOIS или RDAP). Механизм маркировки также может помочь в указании на изменения типа данных в поле (полях) регистрационных данных.
4. Регистраторы должны обеспечить четкое информирование о характере и последствиях идентификации владельца домена в качестве юридического лица. Эти сообщения должны включать:
 - a. Простое и понятное определение юридического лица.
 - b. Разъяснение регистратором владельцу домена (субъекту данных)³ возможных последствий следующих действий:
 - i. Указание на то, что регистрационные данные доменного имени являются данными юридического лица;

² Во избежание неопределенности поясняется, что регистраторы должны предоставить владельцу домена возможность самоидентификации не позднее 15 дней с даты регистрации, если такая возможность не была предоставлена в момент регистрации.

³ Обратите внимание, что владелец домена может не являться субъектом данных, но при любых обстоятельствах соответствующее уведомление/согласие должно предоставляться всем сторонам и всеми сторонами в соответствии с действующим законодательством о защите данных.

- ii. Подтверждение наличия персональных данных или данных, не относящихся к персональным;
 - iii. Выражение согласия⁴. Это также соответствует разделу 3.7.7.4 Соглашения об аккредитации регистраторов (RAA).
5. Если владельцы доменов идентифицируют себя как юридические лица и подтверждают, что их регистрационные данные не содержат персональных данных, то регистраторы должны опубликовать регистрационные данные в общедоступных Службах каталогов регистрационных данных.
 6. Владельцы доменов (субъекты данных) должны иметь простые средства для исправления возможных ошибок.
 7. Проведение различия между владельцами доменов, являющимися юридическими и физическими лицами, само по себе не может быть решающим в вопросе о том, как следует обращаться с информацией (публиковать или скрывать), поскольку данные, предоставленные юридическими лицами, могут содержать персональные данные, защищенные законом о защите данных, например GDPR.

Рекомендация № 3

Группа по EPDP рекомендует, в соответствии с требованиями статьи 40 GDPR к кодексам поведения, принять во внимание вышеуказанные разработанные указания, касающиеся дифференциации юридических и физических лиц, при выполнении в ICANN соответствующими контролерами и обработчиками данных любой возможной будущей работы по составлению Кодекса поведения GDPR. Во избежание разночтений, этот Кодекс поведения является отдельным документом и отличается от Кодекса поведения, упомянутого в RAA и/или Соглашениях об администрировании домена верхнего уровня. В соответствии с преамбулой 99 GDPR, «При разработке кодекса поведения, а также при изменении или дополнении такого кодекса, ассоциации и иные учреждения, представляющие отдельные категории контролеров или обработчиков, должны проконсультироваться с соответствующими заинтересованными сторонами, включая, по возможности, субъектов данных, и принять во внимание полученные при этом предложения и мнения».

Ответ на поручение Совета (b)(i).

Группа по EPDP признает, что использование контактного адреса электронной почты с привязкой к владельцу домена или к регистрации может быть технически осуществимым⁵. Некоторые заинтересованные стороны видят риски и другие проблемы⁶, не позволяющие группе по EPDP дать рекомендацию о введении

⁴ См. также https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

⁵ Некоторые члены группы по EPDP отмечают, что даже при наличии технической возможности для определения общей осуществимости необходимо учесть другие факторы, связанные с необходимыми для реализации такой функции усилиями.

⁶ Например, 1) нет уверенности в том, что работа по реализации такой концепции оправдана потенциальной

требования к сторонам, связанных договорными обязательствами, сделать адрес электронной почты с привязкой к владельцу домена или к регистрации общедоступным в данный момент. Группа по EPDP отмечает, что некоторые группы заинтересованных сторон заявили о преимуществах 1) контактного адреса электронной почты с привязкой к регистрации с точки зрения установления контакта, поскольку высказывались опасения по поводу удобства использования веб-форм, и 2) контактного адреса электронной почты с привязкой к владельцу домена с точки зрения определения взаимосвязи между регистрациями⁷.

Ответ на поручение Совета (b)(ii).

Рекомендация № 4

Группа по EPDP рекомендует сторонам, связанным договорными обязательствами, решившим опубликовать в общедоступной RDDS предполагаемый псевдонимизированный адрес электронной почты, привязанный к владельцу домена или регистрации, изучить юридические рекомендации, полученные группой по EPDP по этому вопросу (см. Приложение F), а также любые другие важные указания, предоставленные соответствующими органами защиты данных.

При оценке рисков, преимуществ и средств защиты, сопряженных с публикацией в общедоступной RDDS предполагаемого псевдонимизированного адреса электронной почты с привязкой к владельцу домена или к регистрации, стороны, связанные договорными обязательствами, должны, как минимум, учитывать следующее:

- Адреса электронной почты физических лиц, привязанные к владельцу домена или регистрации, скорее всего являются персональными данными (то есть ни один из подходов не создает анонимные данные, как они определены в GDPR). Эти данные, вероятно, являются персональными как с точки зрения контролера данных, так и для третьих лиц.
- Однако, даже если такие данные считаются персональными, маскирование адресов электронной почты дает преимущества по сравнению с публикацией реальных адресов электронной почты владельцев доменов, в том числе:
 - (i) демонстрирует принятие мер по повышению конфиденциальности/защите данных по замыслу (статья 25 GDPR); и
 - (ii) несколько снижает риск, связанный с анализом баланса законных интересов при раскрытии маскированного адреса электронной почты третьим лицам.

выгодой. 2) Кроме того, нет уверенности в том, что цели, как они представлены, эффективно или даже наилучшим образом достигаются путем введения требования о наличии адресов электронной почты с привязкой к владельцу домена или к регистрации.

⁷ Возможность определить, какие домены зарегистрировал конкретный владелец, важна для правоохранительных органов и кибербезопасности при расследовании деятельности злоумышленников, которые часто регистрируют множество доменов в злонамеренных целях.

- В целом, публикация адреса электронной почты с привязкой к регистрации, скорее всего, влечет за собой меньший риск, чем публикация адресов электронной почты с привязкой к владельцу домена, из-за объема информации, которую сторона может потенциально связать с субъектом данных на основе контактных адресов электронной почты, привязанных к владельцу домена.
- При публикации адресов электронной почты как с привязкой к владельцу домена, так и с привязкой к регистрации, стороны, связанные договорными обязательствами, должны принять эффективные меры по снижению доступности контактных данных для спамеров.

1.4 Выводы и дальнейшие действия

Настоящий итоговый отчет будет передан Совету GNSO для рассмотрения и утверждения.

1.5 Другие важные разделы этого отчета

Для полного обзора проблем и соответствующих действий группы по EPDP в итоговый отчет включены следующие разделы:

- Общие сведения о рассматриваемых вопросах.
- Перечень участников обсуждений в группе по EPDP, в том числе ведомости посещаемости и ссылки на выражения заинтересованности, где это возможно.
- Приложение, которое содержит мандат группы по EPDP, соответствующий поручениям Совета GNSO.
- Документация по запросам комментариев сообщества через официальные каналы SO/AC и SG/C, в том числе ответы.

2 Подход группы по EPDP

В этом разделе представлен обзор методологии работы и подхода группы по EPDP. Описанные ниже моменты нацелены на то, чтобы читатель получил значимую справочную информацию о дискуссиях и процессах в группе по EPDP, и не должна рассматриваться как полная информация о работе и дискуссиях в группе по EPDP.

2.1 Методология работы

17 декабря 2020 года группа по EPDP начала обсуждение вопросов Фазы 2А. Группа по EPDP вела работу в формате телеконференций, проводимых один или несколько раз в неделю, в дополнение к обмену мнениями по электронной почте через лист рассылки. Материалы всех совещаний группы по EPDP размещены в ее [рабочем вики-пространстве](#), включая [лист рассылки](#), проекты документов, справочные материалы и комментарии, поступившие от организаций поддержки и консультативных комитетов ICANN, в том числе от групп заинтересованных сторон и групп интересов GNSO.

Группа по EPDP также подготовила и передала Совету GNSO план работы в составе [пакета документов по проекту Фазы 2А EPDP](#), который регулярно пересматривался и обновлялся.

2.2 Справочные материалы и подход

Чтобы обеспечить общее понимание тем, которые будут рассматриваться в рамках Фазы 2А, группа поддержки из числа персонала разработала [справочные материалы](#) по каждой из тем. Эти справочные материалы включали следующее: 1) поручения Совета группе по EPDP, 2) соответствующие рекомендации по итогам фаз 1 и 2 EPDP, 3) соответствующие исследования или юридические рекомендации, полученные ранее, 4) процедурные требования, 5) указания по срокам и 6) предлагаемый подход. Перечисленные справочные материалы были распространены среди членов группы по EPDP до начала первого заседания и вместе с обязательными для ознакомления документами легли в основу первого задания группы по EPDP. Говоря конкретнее, группе по EPDP было предложено тщательно изучить указанные исследования и предыдущие юридические рекомендации и подготовить любые уточняющие вопросы.

2.3 Юридический комитет

Как и на Фазах 1 и 2, группа по EPDP полагалась на свой Юридический комитет при рассмотрении и уточнении вопросов, выявленных группой по EPDP. В состав Юридического комитета входит по одному члену от каждой из SG/C/AC, представленных в группе по EPDP.

Юридический комитет Фазы 2А занимался рассмотрением вопросов, предложенных членами группы по EPDP, чтобы гарантировать следующее:

1. вопросы действительно носят юридический характер, в отличие от вопросов политики или ее реализации;
2. вопросы сформулированы беспристрастно, избегая как predetermined результатов, так и позиций конкретных групп интересов;
3. вопросы уместны и своевременны с точки зрения работы группы по EPDP;
4. ограниченный бюджет для привлечения внешнего юрисконсульта используется ответственно.

Юридический комитет распространил все согласованные вопросы среди членов группы по EPDP перед отправкой этих вопросов в компанию Bird & Bird.

На сегодняшний день группа по EPDP приняла решение отправить компании Bird & Bird четыре вопроса по Фазе 2А. Полный текст этих вопросов и полученные в ответ юридические рекомендации приведены в Приложении F.

2.4 Вопросы Совета

При рассмотрении вопросов, поставленных Советом GNSO, группа по EPDP рассмотрела (1) материалы, предоставленные каждой группой в рамках обсуждения; (2) соответствующие материалы фаз 1 и 2; (3) материалы, предоставленные по этим темам каждой группой в ответ на просьбу принять участие на ранних этапах предыдущих фаз, а также соответствующие комментарии, поступившие во время форума общественного обсуждения дополнения к Фазе 2 EPDP⁸; (4) обязательные для прочтения документы по каждой теме, указанные в справочных материалах, включая выполненное корпорацией ICANN исследование «[Дифференциация юридических и физических лиц в службах каталогов регистрационных данных доменных имен \(RDDS\)](#)», и (5) [материалы](#), предоставленные компанией Bird & Bird.

⁸ См. <https://community.icann.org/x/Ag9pBQ>, <https://community.icann.org/x/Ag9pBQ>, <https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en> и [Средство анализа комментариев общественности по дополнению](#).

3 Ответы группы по EPDP на вопросы Совета и ее рекомендации

После рассмотрения результатов общественного обсуждения первоначального отчета группа по EPDP представляет свои ответы и рекомендации на рассмотрение Совета GNSO. В настоящем итоговом отчете указан уровень консенсуса, достигнутый группой по EPDP в отношении различных рекомендаций. Резюме:

Заявление председателя

Хотя данный итоговый отчет и его рекомендации получили единодушную поддержку со стороны группы по EPDP 2А, важно отметить, что некоторые группы сообщества сочли, что работа выполнена в недостаточном объеме или вопросы рассмотрены недостаточно подробно, в то время как другие группы сочли определенные рекомендации нецелесообразными или ненужными. Кроме того, на заключительном этапе нашей работы некоторые группы предпочли бы иметь возможность присвоить более детальные обозначения уровня консенсуса в отношении составных частей рекомендаций. В этом контексте всем читателям итогового отчета по EPDP 2А следует также ознакомиться с представленными каждой группой заявлениями меньшинства, которые прилагаются к итоговому отчету и входят в его состав, и исторической справкой о нашей работе.

Помимо достигнутого в отношении рекомендаций итогового отчета консенсуса есть ряд областей, в которых группы, принимавшие участие в Фазе 2А EPDP, не пришли к полному согласию, включая вопрос о том, должна ли дифференциация регистрационных данных юридических и физических лиц быть обязательной или факультативной, а также вопрос о том, уравнивается ли польза от публикации регистрационных данных юридических лиц риском непреднамеренного раскрытия персональных данных. Рекомендации, содержащиеся в итоговом отчете, практически не повлияли на эти расхождения во мнениях и точках зрения.

Настоящий итоговый отчет представляет собой компромисс, который является максимумом того, что могла достигнуть группа на данный момент в рамках выделенного нам времени и установленного круга задач, и его не следует рассматривать как результат, который полностью удовлетворил всех. Это подчеркивает важность заявлений меньшинства для понимания полного контекста рекомендаций итогового отчета.

Подробнее об этих обозначениях см. в разделе 3.6. [Руководства для Рабочих групп GNSO](#).

• 3.1 Проведение различия между физическими и юридическими лицами

Совет GNSO поставил перед группой по EPDP задачу рассмотреть следующие два вопроса:

- i. Необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»);
- ii. Необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие.

При рассмотрении этих вопросов группа по EPDP начала с анализа всей относящейся к ним информации, включая (1) [исследование](#), проведенное корпорацией ICANN⁹, (2) [юридические рекомендации](#), предоставленные компанией Bird & Bird, и (3) существенный вклад по этой теме во время [форума общественного обсуждения](#). После изучения этой информации группа по EPDP сформулировала ряд уточняющих вопросов, которые после их рассмотрения Юридическим комитетом группы по EPDP были направлены в компанию Bird & Bird (см. <https://community.icann.org/x/xQhACQ>). Группа по EPDP проанализировала [ответы компании Bird & Bird](#) и воспользовалась этой информацией при подготовке приведенных ниже рекомендаций.

• Ответ группы по EPDP на вопрос i.

Группа по EPDP всесторонне обсудила этот вопрос. В качестве отправной точки группа по EPDP отмечает, что GDPR и многие другие законы о защите данных устанавливают требования по защите персональных данных физических лиц. Они не защищают данные юридических лиц, которые не относятся к

⁹ В рамках рекомендации по политике № 17 Фазы 1 группа по EPDP рекомендовала: «Корпорации ICANN необходимо как можно скорее провести исследование, мандат для которого разработан во взаимодействии с сообществом:

- осуществимости дифференцированного подхода к юридическим и физическим лицам и расходов, включая расходы на реализацию и расходы в связи с возможной юридической ответственностью;
- примеров отраслей или других организаций, где используется дифференцированный подход к юридическим и физическим лицам;
- рисков для конфиденциальности владельцев зарегистрированных имен, возникающих в связи с дифференцированным подходом к юридическим и физическим лицам; и
- других потенциальных рисков (если таковые имеются) для регистраторов и регистратур, возникающих в связи с отсутствием дифференцированного подхода».

Корпорация ICANN предоставила результаты [исследования](#) группе по EPDP в июле 2020 года.

персональным¹⁰. В то же время, группа по EPDP признает, что Европейский совет по защите данных (EDPB) в письме от июля 2018 года уведомил ICANN, что «тот факт, что владелец домена является юридическим лицом, сам по себе не обязательно оправдывает неограниченную публикацию персональных данных, относящихся к физическим лицам, которые работают в этой организации или представляют ее», и что «персональные данные, идентифицирующие отдельных сотрудников (или третьих лиц), действующих от имени владельца домена, не должны быть публично доступны по умолчанию в контексте WHOIS»¹¹. Для получения более подробной информации о различных точках зрения на этот вопрос читателям предлагается ознакомиться с первоначальным отчетом группы по EPDP, а также с заявлениями меньшинства, которые прилагаются к данному отчету.

Группа по EPDP дает следующий ответ на поручение Совета оценить необходимость изменения рекомендации по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»):

Группа по EPDP не достигла консенсуса по предлагаемым изменениям рекомендации № 17.1 по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»).

Предложение Совету GNSO

Группа по EPDP признает, что текущие и будущие законодательные изменения могут потребовать дополнительной работы над политикой в этой области, например, для разрешения потенциальных конфликтов с существующими требованиями политики и/или для рассмотрения вопроса о том, существует ли риск сегментации рынка, который необходимо устранить. В то же время, группа по EPDP признает, что до принятия законодательства, возможно, не удастся точно оценить его влияние. Группа по EPDP рекомендует Совету GNSO следить за этими событиями через отчеты о ситуации в законодательной/нормативной сфере, которые публикует корпорация ICANN.

¹⁰ «Эти положения не распространяются на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица».

¹¹ Андреа Елинек (Andrea Jelinek), Европейский совет по защите данных, письмо Йорану Марби (Goran Marby) от 5 июля 2018 года, доступно по ссылке <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

Отмечая текущие обсуждения и ожидаемое принятие уточненной редакции Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем (NIS2), группа по EPDP настоятельно рекомендует Совету GNSO согласно существующим процедурам определить рамки возможной будущей работы в области политики после принятия NIS2, чтобы оценить, считается ли желательной и/или необходимой дальнейшая разработка политики.

Указания по дифференциации

Группа по EPDP признает, что может возникнуть необходимость в облегчении и гармонизации практики для тех сторон, связанных договорными обязательствами, которые решили проводить различие между юридическими и физическими лицами.

Чтобы облегчить дифференциацию, группа по EPDP разработала указания, которые приведены в разделе ниже. В данных указаниях группа по EPDP предлагает регистраторам рассмотреть возможность использования поля, которое будет указывать на тип соответствующего владельца домена (юридическое или физическое лицо) и тип данных владельцев доменов-юридических лиц, которых это затрагивает (персональные данные или данные, не являющиеся персональными). Эта концепция определения типа регистрационных данных доменных имен также упоминается в рекомендации № 9.4.4 Фазы 2 EPDP (автоматизированный ответ на запросы о раскрытии информации).

В следующей рекомендации группа по EPDP описывает, как сторона, связанная договорными обязательствами, желающая дифференцировать данные, может сделать это с помощью нового поля или полей для фиксации результатов такой дифференциации.

Рекомендация № 1

Группа по EPDP рекомендует **ОБЯЗАТЕЛЬНО** создать поле или поля, чтобы способствовать дифференциации регистрационных данных юридических и физических лиц и/или определению наличия персональных данных в составе регистрационных данных. Корпорация ICANN **ДОЛЖНА** координировать свои действия с техническим сообществом, например с Рабочей группой по RDAP, для разработки всех необходимых стандартов, связанных с использованием этого поля или полей в EPP и RDDS.

Такое поле или поля **МОГУТ** использоваться сторонами, связанными договорными обязательствами, которые разграничивают регистрационные данные юридических и физических лиц и/или указывают, входят ли в состав регистрационных данных персональные данные или нет. Во избежание неопределенности поясняется, что стороны, связанные договорными обязательствами, **МОГУТ** использовать

указанное поле (поля). Это означает, что, если сторона, связанная договорными обязательствами, принимает решение не использовать такое поле, оно может быть оставлено пустым или отсутствовать. Кроме того, стороны, связанные договорными обязательствами, МОГУТ включить это поле (поля) в ответ RDDS.

SSAD, в соответствии с рекомендациями по итогам Фазы 2 EPDP, ДОЛЖНА поддерживать такое поле или поля для содействия интеграции между SSAD и системами сторон, связанных договорными обязательствами. Это поле (поля) должно быть способно вместить следующие значения:

Правовой статус

- Разграничение по правовому статусу не проводилось (значение по умолчанию)
- Не указано — свидетельствует, что это не указано владельцем зарегистрированного имени и/или регистратором
- Владелец зарегистрированного имени является физическим лицом
- Владелец зарегистрированного имени является юридическим лицом

Персональные данные

- Наличие персональных данных не определялось (значение по умолчанию)
- Не указано — свидетельствует, что это не указано владельцем зарегистрированного имени и/или регистратором
- Регистрационные данные содержат персональную информацию
- Регистрационные данные НЕ содержат персональную информацию

• Ответ группы по EPDP на вопрос ii.

Группа по EPDP приступила к решению задачи с рассмотрения того, какие указания принесли бы пользу регистраторам и операторам регистратур, решившим разграничить регистрации юридических и физических лиц.

Определения (обратите внимание, что они позаимствованы из предыдущих работ в области EPDP, как указано ниже):

- EPDP-p1-IRT¹²: «Публикация», «публиковать» и «опубликованный» означает предоставление регистрационных данных в общедоступных службах каталогов регистрационных данных.
- EPDP-p1-IRT¹³: «Регистрационные данные» означают значения элементов данных, полученные от физического или юридического лица или созданные регистратором или оператором регистратуры, в обоих случаях в связи с зарегистрированным именем в соответствии с разделом 7 настоящей Политики.

¹² См. https://docs.google.com/document/d/1SVFkol6RmrVVz--RrVLSOj1bmz1qLb7_JTuv7At4Uo/edit.

¹³ Тот же источник.

- Итоговый отчет EPDP-P1¹⁴: «Раскрытие» означает действие по обработке данных, позволяющее контролеру взять на себя ответственность за разглашение персональных данных третьим сторонам по запросу.

Справочная информация и наблюдения группы по EPDP

Разрабатывая приведенные ниже указания, группа по EPDP хотела бы напомнить Совету и более широкому сообществу о следующем:

Сфера применения GDPR и других законов о защите данных

- A. GDPR и другие законы о защите данных устанавливают требования к защите персональных данных физических лиц. Они не защищают персональные данные юридических лиц и данные, не являющиеся персональными.
- B. Действие GDPR не распространяется на обработку персональных данных юридических лиц и частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица. Однако, когда в связи с юридическим лицом используется информация о физическом лице, например о представителе бизнеса, данные этого физического лица остаются защищенными как персональные данные в соответствии с GDPR.
- C. Проведение различия между владельцами доменов, являющимися юридическими и физическими лицами, не может быть решающим в вопросе о том, как следует обращаться с информацией (публиковать или скрывать), поскольку данные, предоставленные юридическими лицами, могут содержать персональные данные, защищенные законом о защите данных, например GDPR.
- D. Хотя GDPR не распространяется на обработку персональных данных, касающихся юридических лиц, принципы GDPR, часть которых описана ниже, все же могут применяться, если персональные данные физического лица обрабатываются в рамках процесса дифференциации, и по мере необходимости должны учитываться сторонами, связанными договорными обязательствами. В соответствии с принципами, изложенными в статье 5 GDPR:
 - a. Законность, справедливость и прозрачность: «Любая обработка персональных данных должна быть законной, справедливой и прозрачной. Физические лица должны четко понимать, что их персональные данные собираются, используются или иным образом обрабатываются, и в каком объеме эти персональные данные обрабатываются или будут обрабатываться». Принцип прозрачности «касается, в частности, информации для субъектов данных о личности контролера и целях обработки¹⁵[.] [. . .]

¹⁴ См. <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf>.

¹⁵ См. указания Ирландской комиссии по защите данных в отношении права на получение информации. (<https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-1-4->

Если правовой основой является согласие, то предоставление информации субъектам данных до получения их согласия необходимо для того, чтобы они могли принимать обоснованные решения, понимать, на что соглашаются, и, например, реализовать свое право на отзыв согласия»¹⁶.

- b. Ограничение целей: «Персональные данные должны [. . .] собираться для указанных, очевидных и легитимных целей и не обрабатываться дополнительно каким-либо способом, не совместимым с этими целями».¹⁷
- c. Минимизация данных: «Ограничить объем собираемых персональных данных тем, что необходимо для достижения цели»¹⁸.
- d. Подотчетность: Принцип подотчетности GDPR «требует от организаций демонстрировать (и в большинстве случаев документировать), каким образом они соблюдают принципы защиты данных при ведении бизнеса»¹⁹.

Соответствующие рекомендации Фазы 1 EPDP²⁰

- E. Согласно рекомендации № 6 Фазы 1 EPDP²¹, «Регистратор должен в минимальный коммерчески приемлемый срок предоставить владельцу зарегистрированного имени возможность дать согласие на опубликование вымаранных контактных данных, а также адреса электронной почты, в RDS ответственного регистратора».
- F. Согласно рекомендации № 17 Фазы 1 EPDP, «Регистраторам и операторам регистратур разрешено, но не вменяется в обязанность проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами».

[gdpr](#)) и статья 29 Руководства для рабочих групп по транспарентности согласно Регламенту 2016/679, разделы 6 и 7 (принятого EDPB) (<https://ec.europa.eu/newsroom/article29/items/622227>).

¹⁶ См. Руководство EDPB, 05/2020, принципы получения согласия в соответствии с регламентом 2016/679, раздел 3.3.

¹⁷ См. GDPR, статья 5(1)(b); см. также руководство Управления комиссара по информации Великобритании по ограничению целей, (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>).

¹⁸ См. Руководство EDPB, 04/2019, защита данных по замыслу и по умолчанию, раздел 3.5 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf) и GDPR, статья 5.1 (c).

¹⁹ См.: указания Ирландской комиссии по защите данных в отношении подотчетности (<https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation>); см. также Руководство EDPB, 04/2019, защита данных по замыслу и по умолчанию, раздел 3.9 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

²⁰ Обратите внимание, что рекомендация № 12 Фазы 1 EPDP, касающаяся поля «Организация», после ее выполнения может также помочь сторонам, связанным договорными обязательствами, в проведении различия между юридическими и физическими лицами, если они решат это сделать.

²¹ Подробнее о ходе выполнения рекомендаций Фазы 1 EPDP см. по ссылке <https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en>.

Соответствующие рекомендации Фазы 2 EPDP

- Г. Согласно рекомендации № 9.4.4 итогового отчета по Фазе 2²², которая касается автоматизации обработки в SSAD: «Группа по EPDP рекомендует **ОБЯЗАТЕЛЬНО** автоматизировать с момента запуска SSAD следующие типы запросов о раскрытии данных, для которых юридическая допустимость полной автоматизации (прием и обработка решения о раскрытии) зафиксирована в GDPR[.] [. . .] Отсутствие персональных данных в регистрационной записи, которая ранее была раскрыта стороной, связанной договорными обязательствами». Данная рекомендация 9.4.4 в целом посвящена автоматизации раскрытия информации для регистрационных записей, которые не содержат персональных данных²³.
- Н. Согласно рекомендации № 8.7.1 итогового отчета по Фазе 2, если сторона, связанная договорными обязательствами, получает запрос от программы управления центральным шлюзом SSAD и определяет, что это действительный запрос, «если после оценки основных данных сторона, связанная договорными обязательствами, обоснованно определяет, что раскрытие запрошенных элементов данных не приведет к раскрытию персональных данных, сторона, связанная договорными обязательствами, **ДОЛЖНА** раскрыть данные, если только раскрытие не запрещено применимым законодательством».

Бизнес-модели регистраторов

- И. Регистраторы используют различные бизнес-модели (розничная торговля, оптовая торговля, защита бренда, другие), и универсальные или слишком директивные указания могут не учитывать должным образом весь спектр бизнес-моделей регистраторов и различные технологические процессы, которые могут требоваться различным бизнес-моделям. Вместо этого любые указания должны обеспечивать гибкость, позволяющую регистраторам внедрить такой дифференцированный подход, который наилучшим образом соответствует их бизнес-модели и снижает риски, связанные с дифференциацией, до приемлемого для конкретного регистратора уровня. Например, дифференциация в момент регистрации не всегда может быть уместной, в том числе для некоторых бизнес-моделей регистраторов.

²² Обратите внимание, что рекомендации Фазы 2 EPDP находятся на рассмотрении/утверждении Правления ICANN.

²³ Обратите внимание, что точные детали того, как будет выполняться эта рекомендация, должны быть определены корпорацией ICANN в сотрудничестве с Группой по проверке выполнения рекомендаций после утверждения рекомендаций Правлением ICANN.

Предложенные указания

Рекомендация № 2

Группа по EPDP считает, что связанным договорными обязательствами сторонам, решившим проводить дифференциацию по типу лица, СЛЕДУЕТ выполнять приведенные ниже указания²⁴ и четко документировать все этапы обработки данных. Однако в задачи и обязанности группы по EPDP не входит принятие окончательного решения в отношении юридических рисков, поскольку такая ответственность в конечном итоге лежит на контролере (контролерах) данных. GDPR защищает права физических лиц в сфере обработки их персональных данных. Действие GDPR не распространяется на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица. [Преамбула 14, GDPR] Это обычно позволяет раскрывать данные юридических лиц, поскольку они не входят в сферу действия GDPR; однако при обработке данных юридических лиц стороны, связанные договорными обязательствами, должны принять меры предосторожности, чтобы избежать разглашения данных, позволяющих идентифицировать физическое лицо, в составе данных, обозначенных как данные юридического лица, поскольку это пример информации, которая *входит* в сферу действия GDPR. Подробнее об этом различии см. в [письме](#) Европейского совета по защите данных, начиная со стр. 4.

1. Владельцам доменов следует разрешить самостоятельно идентифицировать себя как физическое или юридическое лицо. Регистраторы должны предоставить владельцам доменов эту возможность самоидентификации в качестве физических или юридических лиц (i) в момент регистрации или без неоправданной задержки после регистрации²⁵ и (ii) в момент обновления владельцем домена контактной информации или без неоправданной задержки после обновления контактной информации.
2. Любой процесс дифференциации должен гарантировать вымарывание данных физических лиц из общедоступной RDDS за исключением случаев, когда субъект данных дал согласие на публикацию этих данных или они могут быть опубликованы на другом законном основании согласно GDPR в соответствии с подходом «защита данных по замыслу и по умолчанию», изложенным в статье 25 GDPR.

²⁴ Обратите внимание, что представители корпорации ICANN предоставили группе по EPDP следующую информацию о том, как эти указания будут реализованы после их одобрения:
<https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html>.

²⁵ Во избежание неопределенности поясняется, что регистраторы должны предоставить владельцу домена возможность самоидентификации не позднее 15 дней с даты регистрации, если такая возможность не была предоставлена в момент регистрации.

3. В рамках внедрения регистраторам следует рассмотреть возможность использования поля (полей), описанного в рекомендации № 1, в RDDS, SSAD или их собственных наборах данных, где будет указан тип соответствующего лица (физическое или юридическое), а в случае юридического лица также и тип соответствующих данных (персональные или не относящиеся к персональным). Такая маркировка могла бы содействовать рассмотрению запросов на раскрытие информации и выполнению требований по автоматизации SSAD и предоставлению данных юридических лиц, не относящихся к персональным, системами, отличными от SSAD (такими как WHOIS или RDAP). Механизм маркировки также может помочь в указании на изменения типа данных в поле (полях) регистрационных данных.
4. Регистраторы должны обеспечить четкое информирование о характере и последствиях идентификации владельца домена в качестве юридического лица. Эти сообщения должны включать:
 - c. Простое и понятное определение юридического лица.
 - d. Разъяснение регистратором владельцу домена (субъекту данных)²⁶ возможных последствий следующих действий:
 - i. Указание на то, что регистрационные данные доменного имени являются данными юридического лица;
 - ii. Подтверждение наличия персональных данных или данных, не относящихся к персональным;
 - iii. Выражение согласия²⁷. Это также соответствует разделу 3.7.7.4 Соглашения об аккредитации регистраторов (RAA).
5. Если владельцы доменов идентифицируют себя как юридические лица и подтверждают, что их регистрационные данные не содержат персональных данных, то регистраторы должны опубликовать регистрационные данные в общедоступных Службах каталогов регистрационных данных.
6. Владельцы доменов (субъекты данных) должны иметь простые средства для исправления возможных ошибок.
7. Проведение различия между владельцами доменов, являющимися юридическими и физическими лицами, само по себе не может быть решающим в вопросе о том, как следует обращаться с информацией (публиковать или скрывать), поскольку данные, предоставленные юридическими лицами, могут содержать персональные данные, защищенные законом о защите данных, например GDPR.

Рекомендация № 3

Группа по EPDP рекомендует, в соответствии с требованиями статьи 40 GDPR к кодексам поведения, принять во внимание вышеуказанные разработанные указания, касающиеся дифференциации юридических и физических лиц,

²⁶ Обратите внимание, что владелец домена может не являться субъектом данных, но при любых обстоятельствах соответствующее уведомление/согласие должно предоставляться всем сторонам и всеми сторонами в соответствии с действующим законодательством о защите данных.

²⁷ См. также https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

при выполнении в ICANN соответствующими контролерами и обработчиками данных любой возможной будущей работы по составлению Кодекса поведения GDPR. Во избежание разночтений, этот Кодекс поведения является отдельным документом и отличается от Кодекса поведения, упомянутого в RAA и/или Соглашениях об администрировании домена верхнего уровня. В соответствии с преамбулой 99 GDPR, «При разработке кодекса поведения, а также при изменении или дополнении такого кодекса, ассоциации и иные учреждения, представляющие отдельные категории контролеров или обработчиков, должны проконсультироваться с соответствующими заинтересованными сторонами, включая, по возможности, субъектов данных, и принять во внимание полученные при этом предложения и мнения».

Три примера сценариев

(Обратите внимание, что эти сценарии призваны проиллюстрировать, как регистратор может применить вышеперечисленные принципы. Эти сценарии НЕ должны рассматриваться как указания сами по себе).

Группа по EPDP определила три различных высокоуровневых сценария того, как может происходить дифференциация в зависимости от ответственных лиц и сроков такой дифференциации. Следует отметить, что возможны и другие подходы и/или их сочетание.

1. Самоидентификация субъекта данных во время сбора данных/регистрации

- a. Регистратор информирует владельца домена (согласно указанию №3 выше) и просит владельца домена (субъекта данных) указать тип (юридическое или физическое лицо) в момент сбора регистрационных данных. В случае юридического лица регистратор также должен запросить у владельца домена подтверждение того, что предоставлены только данные, не являющиеся персональными²⁸.
- b. Если владелец домена (субъект данных) самоидентифицировался как юридическое лицо и представил подтверждение того, что регистрационные данные не содержат персональных данных, регистратор должен (i) связаться по предоставленным контактным данным для проверки заявления владельца домена²⁹; (ii) обеспечить автоматизированное раскрытие этой группы

²⁸ Обратите внимание, что подтверждение отсутствия персональных данных также может быть получено позднее. Однако, пока владелец домена не подтвердит отсутствие персональных данных в регистрационных данных, регистратор не осуществляет автоматизированное раскрытие этих регистрационных данных.

²⁹ Согласно [указанию](#) Bird & Bird, «такой метод верификации предпочтителен и позволит снизить риск. Это снижение риска будет наиболее значительным при наличии разумного льготного периода, позволяющего подать возражение до публикации данных, о которых идет речь, в составе регистрационных данных», а «требование дать **утвердительный** ответ на проверочное письмо представляется чрезмерно осторожным, пока исследования не покажут, что принятые меры не позволяют предотвратить попадание очень значительных объемов персональных данных в опубликованные регистрационные данные. Однако в случае возврата проверочного электронного письма (то есть сторона, связанная договорными обязательствами, знает, что оно не было доставлено) лучше воздержаться от публикации».

регистрационных данных в ответ на запросы SSAD; (iii) опубликовать данные (предоставить регистрационные данные в общедоступных Службах каталогов регистрационных данных).

- c. Если владелец домена (субъект данных) самоидентифицировался как физическое лицо или подтвердил наличие персональных данных, регистратор обеспечивает автоматизированное раскрытие и публикацию регистрационных данных только в том случае, если субъект данных дал согласие на публикацию³⁰.

2. Самоидентификация субъекта данных при обновлении регистрации³¹

- a. Регистратор собирает регистрационные данные и временно скрывает их.
- b. Регистратор информирует владельца домена (согласно указанию № 3 выше) и просит владельца домена (субъекта данных) самоидентифицироваться как юридическое или физическое лицо. Регистратор также должен попросить владельца домена, идентифицирующего себя как юридическое лицо, подтвердить, что персональные данные не были предоставлены³².
- c. Владелец домена (субъект данных) самостоятельно идентифицирует себя как юридическое или физическое лицо и подтверждает отсутствие персональных данных после завершения обновления. Например, владелец домена может подтвердить тип лица при первоначальной проверке данных, в ответ на получение электронного письма с напоминанием о данных WHOIS для существующих регистраций или через отдельное уведомление с просьбой о самоидентификации³³.
- d. Если субъект данных самоидентифицируется как юридическое лицо и подтверждает, что регистрационные данные не содержат персональных данных, регистратор должен (i) связаться по предоставленным контактным данным для проверки заявления владельца домена³⁴; (ii) обеспечить автоматизированное раскрытие этой группы регистрационных данных в ответ на запросы SSAD; и (iii) опубликовать данные.

³⁰ Обратите внимание, что субъект данных может не быть стороной, осуществляющей процесс, но может попросить об этом третью сторону. В таких обстоятельствах документирование согласия может оказаться невозможным.

³¹ Ожидается, что для этого сценария будут соблюдены сроки, аналогичные тем, которые в настоящее время применяются в Спецификации программы обеспечения точности данных WHOIS Соглашения об аккредитации регистраторов (см. <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy>).

³² Обратите внимание, что подтверждение отсутствия персональных данных также может быть получено позднее. Однако, пока владелец домена не подтвердит отсутствие персональных данных в регистрационных данных, регистратор не осуществляет автоматизированное раскрытие этих регистрационных данных.

³³ Обратите внимание, что выполнение рекомендации № 12 (Поле «Организация») Фазы 1 EPDP может облегчить процесс самоидентификации.

³⁴ Согласно [указаниям](#) Bird & Bird, «такой метод верификации предпочтителен и позволит снизить риск. Это снижение риска будет наиболее значительным при наличии приемлемого льготного периода, позволяющего подать возражение до публикации данных, о которых идет речь, в составе регистрационных данных», а «требование дать утвердительный ответ на проверочное письмо представляется чрезмерной осторожностью, пока исследования не покажут, что принятые меры не позволяют предотвратить попадание очень значительных объемов персональных данных в опубликованные регистрационные данные. Однако в случае возврата проверочного электронного письма (то есть сторона, связанная договорными обязательствами, знает, что оно не было доставлено) лучше воздержаться от публикации».

3. Определение регистратором типа владельца домена на основании предоставленных данных

- a. Регистратор собирает регистрационные данные и временно скрывает их.
- b. На основании предоставленных данных регистратор делает вывод о том, какое это лицо: юридическое или физическое³⁵.
- c. Если регистратор сделал вывод, что это юридическое лицо, а затем проинформировал владельца домена (субъекта данных) (согласно указанию № 3 выше) и убедился в отсутствии персональных данных, регистратор должен (i) связаться по предоставленным контактным данным для проверки заявления владельца домена³⁶, (ii) обеспечить автоматизированное раскрытие этой группы регистрационных данных в ответ на запросы SSAD и (iii) опубликовать данные.
- d. Если регистратор сделал вывод, что владелец домена является физическим лицом, или обнаружил персональные данные, регистратор не должен раскрывать регистрационные данные, за исключением случаев, когда владелец домена дал согласие на их публикацию или регистратор раскрывает данные в ответ на законное требование о раскрытии.

Группа по EPDP признает, что во всех вышеперечисленных сценариях существует возможность неправильной идентификации, что может привести к непреднамеренному раскрытию персональных данных. В связи с этим группа по EPDP рекомендует ознакомиться с [меморандумом Bird & Bird](#), который также можно найти в Приложении F, особенно с разделами 11.1-2, 13, 14.3 и 18.

• 3.2 Возможность индивидуальных контактов

Совет GNSO поставил перед группой по EPDP задачу рассмотреть следующие два вопроса:

- i. Имеется ли возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, и если да, должно ли это стать требованием.
- ii. Если это осуществимо, но не является требованием, какие указания следует дать связанным договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты.

³⁵ Некоторые члены группы по EPDP отметили, что при осуществлении дифференциации без участия владельца домена (субъекта данных) могут возникнуть риски для регистратора.

³⁶ Согласно [указаниям Bird & Bird](#), «такой метод верификации предпочтителен и позволит снизить риск. Это снижение риска будет наиболее значительным при наличии приемлемого льготного периода, позволяющего подать возражение до публикации данных, о которых идет речь, в составе регистрационных данных», а «требование дать утвердительный ответ на проверочное письмо представляется чрезмерной осторожностью, пока исследования не покажут, что принятые меры не позволяют предотвратить попадание очень значительных объемов персональных данных в опубликованные регистрационные данные. Однако в случае возврата проверочного электронного письма (то есть сторона, связанная договорными обязательствами, знает, что оно не было доставлено) лучше воздержаться от публикации».

Совет также указал, что «группы, запросившие дополнительное время для рассмотрения указанной темы, к которым относятся ALAC, GAC и SSAC, должны будут представить конкретные предложения по этому вопросу»³⁷.

Рассмотрение этих вопросов группа по EPDP начала с анализа [юридических рекомендаций](#), полученных в ходе Фазы 1, и рассмотрела возможные предложения, которые могли бы обеспечить достаточную защиту для решения проблем, отмеченных в юридическом меморандуме.

Группа по EPDP отметила, что использование анонимизированного адреса электронной почты влияет на необходимые средства защиты и возможные последствия для субъектов данных, а значит, и на целесообразность. Группа рассмотрела последствия и преимущества двух вариантов использования такого контакта в соответствии с двумя различными целями, заявленными сторонниками индивидуальных контактов, а именно: 1) возможность быстро и эффективно связаться с владельцем домена и 2) корреляция между доменами, зарегистрированными одним и тем же владельцем.

Группа по EPDP также отметила, что используемая в контексте данного обсуждения терминология могла бы выиграть от дополнительного уточнения. Группа по EPDP поручила Юридическому комитету предложить обновленную терминологию и проанализировать уточняющие вопросы для отправки в компанию Bird & Bird. Юридический комитет предложил набор рабочих определений, которые представил группе по EPDP 23 февраля 2021 года (см. [здесь](#)). Кроме того, Юридический комитет подготовил и передал компании Bird & Bird ряд уточняющих вопросов, на которые компания Bird & Bird [ответила](#) 9 апреля 2021 года. Группа по EPDP приняла во внимание эти юридические рекомендации при составлении своего ответа на вопросы Совета.

Определения

После первоначального рассмотрения первого вопроса своего устава группа по EPDP отметила, что термин «анонимный» в этом вопросе был использован неправильно. Группа по EPDP отметила, что анонимизация данных, действительно соответствующая GDPR, подразумевает невозможность идентификации субъекта данных «ни контролером, ни любым другим лицом» ни прямо, ни косвенно. (См. GDPR, статья 26.) Исходя из этого понимания, группа по EPDP решила сосредоточиться в своем вопросе на псевдонимизации данных и дополнительно уточнила определения в своих последующих вопросах к компании Bird & Bird.

«Контактный адрес электронной почты с привязкой к владельцу домена» означает «адрес электронной почты для всех доменов, зарегистрированных уникальным

³⁷ <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf>

владельцем [у данного регистратора] ИЛИ [у разных регистраторов]³⁸, используемый в качестве псевдонимных³⁹ данных при обработке сторонами, не связанными договорными обязательствами^{40,41}.

«Контактный адрес электронной почты с привязкой к регистрации» означает «отдельный адрес электронной почты однократного применения для каждого доменного имени, зарегистрированного уникальным владельцем, используемый в качестве анонимных данных при обработке сторонами, не связанными договорными обязательствами». ⁴²

Однако следует отметить, что компания Bird & Bird, даже принимая эти определения, сообщила, что контактная электронная почта с привязкой к владельцу домена или регистрации создает «высокую вероятность того, что публикация или автоматизированное раскрытие таких адресов электронной почты будет считаться обработкой персональных данных».

Справочная информация и наблюдения группы по EPDP

Подготавливая ответ на вопросы Совета, группа по EPDP хотела бы напомнить Совету и более широкому сообществу о следующем:

³⁸ Юридическому комитету было поручено проанализировать юридические рекомендации, полученные в ходе Фазы 2, и определить, необходимы ли дополнительные юридические рекомендации. В качестве первого вопроса Юридический комитет решил уточнить терминологию, использованную в [вопросе Фазы 2](#); в частности, вместо терминов «анонимизация» и «псевдонимизация» Юридический комитет согласился использовать термины «контактная электронная с привязкой к регистрации» и «контактная электронная почта с привязкой к владельцу домена», поскольку группа по EPDP отметила, что предыдущее использование термина «анонимизация» не соответствует определению анонимности в GDPR. При разработке новых определений Юридический комитет отметил, что контакт с привязкой к владельцу домена может существовать в рамках одного ответственного регистратора ИЛИ у всех регистраторов. Однако Юридический комитет решил, что вопрос о том, должен ли контакт с привязкой к владельцу домена существовать в рамках ответственного регистратора или у разных регистраторов, является вопросом политики для группы по EPDP, а не правовым вопросом для Юридического комитета или Bird & Bird. Соответственно, Юридический комитет решил оставить оба варианта в скобках, а компания Bird & Bird в [меморандуме Фазы 2А](#) высказала свое мнение о законности и сопутствующих рисках обоих вариантов.

³⁹ Некоторые члены группы по EPDP считают, что термин «псевдонимный» нужно заменить на «анонимный». Однако следует отметить, что представленное выше определение было включено в вопрос к компании Bird & Bird и фигурировало в полученных от нее указаниях.

⁴⁰ Некоторые члены группы по EPDP считают, что слова «стороны, не связанные договорными обязательствами» следует заменить на «стороны, не являющиеся контролерами». Однако следует отметить, что представленное выше определение было включено в вопрос к компании Bird & Bird и фигурировало в полученных от нее указаниях.

⁴¹ Некоторые члены группы по EPDP предложили расширить определение, включив в него «ИЛИ [во всех TLD, находящихся под управлением одного и того же провайдера услуг регистратур]». Однако следует отметить, что представленное выше определение было включено в вопрос к компании Bird & Bird и фигурировало в полученных от нее указаниях.

⁴² Некоторые члены группы по EPDP считают, что слова «стороны, не связанные договорными обязательствами» следует заменить на «стороны, не являющиеся контролерами». Однако следует отметить, что представленное выше определение было включено в вопрос к компании Bird & Bird и фигурировало в полученных от нее указаниях.

Приложение к Временной спецификации («Важные вопросы для рассмотрения сообществом»)

- Принятая Правлением ICANN 17 мая 2018 года [Временная спецификация для регистрационных данных в gTLD](#) содержала следующую формулировку в приложении под названием «Важные вопросы для рассмотрения сообществом»:

«Рассмотрение возможности ввести требование об использовании единообразного анонимизированного адреса электронной почты для всех доменных имен, зарегистрированных у конкретного регистратора, обеспечивая при этом безопасность/стабильность и выполняя требования раздела 2.5.1 Приложения А».

Для справки, раздел 2.5.1 в Приложении А гласит: «Регистратор ДОЛЖЕН предоставить адрес электронной почты или веб-форму, чтобы способствовать связи по электронной почте с соответствующим контактным лицом, но НЕ ДОЛЖЕН указывать адрес электронной почты контактного лица или само контактное лицо».

Соответствующие рекомендации Фазы 1 EPDP

Рекомендация № 6 EPDP-P1

Группа по EPDP рекомендует обязать Регистратора, в минимальный коммерчески приемлемый срок, предоставить Владельцу зарегистрированного имени возможность дать Согласие на опубликование вымаранных контактных данных, а также адреса электронной почты, в RDS ответственного регистратора.

Рекомендация № 13 EPDP-P1

1) Согласно рекомендации группы по EPDP, Регистратор ДОЛЖЕН предоставить адрес электронной почты или веб-форму, чтобы способствовать связи по электронной почте с соответствующим контактным лицом, но НЕ ДОЛЖЕН указывать адрес электронной почты контактного лица или само контактное лицо, если Владелец зарегистрированного имени не дал согласия на опубликование своего адреса электронной почты в соответствии с Рекомендацией № 6.

2) Согласно рекомендации группы по EPDP, Регистратор ДОЛЖЕН хранить журналы событий, в которых отсутствуют персональные данные, но содержатся данные, подтверждающие пересылку сообщений между отправителем запроса и Владельцем зарегистрированного имени без указания отправителя, получателя или содержания сообщений. Такие регистрационные записи по запросу будут предоставляться ICANN для целей контроля за соблюдением обязательств. Эта рекомендация никоим образом не препятствует принятию регистратором

разумных и целесообразных мер по предотвращению злоупотребления его процедурой установления связи⁴³.

*Обратите внимание, что во время обсуждения на Фазе 2А некоторые члены группы по EPDP подняли вопрос о веб-формах и потенциальных проблемах, связанных с использованием таких веб-форм. Было отмечено следующее: хотя возможность использования веб-формы предусмотрена в рекомендации № 13 по итогам Фазы 1 EPDP, это требование совпадает с требованиями Временной спецификации, вступившей в силу 25 мая 2018 года. Консультации с корпорацией ICANN показали, что веб-формы не были значительным источником жалоб, и этот вопрос не поднимался в качестве проблемы в контексте Группы по проверке выполнения рекомендаций, которой поручено выполнить эту рекомендацию Фазы 1⁴⁴. По мнению некоторых членов группы, такие проблемы, даже если они существуют, не входят в сферу компетенции группы по EPDP, учитывая ее ограниченные полномочия. Группа по EPDP не смогла прийти к соглашению о дальнейших действиях в этой области.

Рекомендация № 14 EPDP-P1

Если при регистрации доменного имени используется услуга «аффилированной» организации по сохранению конфиденциальности/регистрации через доверенных лиц (например, когда данные о физическом лице скрываются), Регистратор (и, при необходимости, Регистратура) ДОЛЖЕН опубликовать в открытой системе RDDS и отправлять в ответ на любой запрос полный набор данных RDDS поставщика услуг сохранения конфиденциальности/регистрации через доверенных лиц, не являющихся персональными, в состав которого МОЖЕТ также входить псевдонимизированный адрес электронной почты этого поставщика.

Рассмотрение этой темы в рамках Фазы 2 EPDP

В окончательном отчете по итогам работы группы по EPDP над Фазой 2 сказано:

«Возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов: Группа по EPDP получила юридические рекомендации, в которых говорится, что публикация единообразных маскированных адресов электронной почты приводит к публикации персональных данных; это говорит о том, что широкое опубликование маскируемых адресов электронной почты в настоящее время не представляется возможным в рамках GDPR. Дальнейшая работа по этому вопросу рассматривается Советом GNSO».

⁴³ Например, к таким злоупотреблениям относится, помимо прочего, умышленная отправка в систему регистратора огромного количества объемных запросов с указанием недействительных контактных данных. Эта рекомендация не направлена на создание препятствий для отправки законных запросов.

⁴⁴ См. <https://community.icann.org/x/I4GBCQ>.

Предлагаемые ответы группы по EPDP на вопросы Совета

- i. Имеется ли возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, и если да, должно ли это стать требованием.
- ii. Если это осуществимо, но не является требованием, какие указания следует дать связанным договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты.

• Ответ группы по EPDP на вопрос i.

Группа по EPDP признает, что использование контактного адреса электронной почты с привязкой к владельцу домена или к регистрации может быть технически осуществимым⁴⁵. Некоторые заинтересованные стороны видят риски и другие проблемы⁴⁶, не позволяющие группе по EPDP дать рекомендацию о введении требования к сторонам, связанных договорными обязательствами, сделать адрес электронной почты с привязкой к владельцу домена или к регистрации общедоступным в данный момент. Группа по EPDP отмечает, что некоторые группы заинтересованных сторон заявили о преимуществах 1) контактного адреса электронной почты с привязкой к регистрации с точки зрения установления контакта, поскольку высказывались опасения по поводу удобства использования веб-форм, и 2) контактного адреса электронной почты с привязкой к владельцу домена с точки зрения определения взаимосвязи между регистрациями⁴⁷.

• Ответ группы по EPDP на вопрос ii.

Рекомендация № 4

Группа по EPDP рекомендует сторонам, связанным договорными обязательствами, решившим опубликовать в общедоступной RDDS предполагаемый псевдонимизированный адрес электронной почты, привязанный к владельцу домена или регистрации, изучить юридические рекомендации, полученные группой по EPDP по этому вопросу (см. Приложение F), а также любые другие важные указания, предоставленные соответствующими органами защиты данных.

⁴⁵ Некоторые члены группы по EPDP отмечают, что даже при наличии технической возможности для определения общей осуществимости необходимо учесть другие факторы, связанные с необходимыми для реализации такой функции усилиями.

⁴⁶ Например, 1) нет уверенности в том, что работа по реализации такой концепции оправдана потенциальной выгодой. 2) Кроме того, нет уверенности в том, что цели, как они представлены, эффективно или даже наилучшим образом достигаются путем введения требования о наличии адресов электронной почты с привязкой к владельцу домена или к регистрации.

⁴⁷ Возможность определить, какие домены зарегистрировал конкретный владелец, важна для правоохранительных органов и кибербезопасности при расследовании деятельности злоумышленников, которые часто регистрируют множество доменов в злонамеренных целях.

При оценке рисков, преимуществ и средств защиты, сопряженных с публикацией в общедоступной RDDS предполагаемого псевдонимизированного адреса электронной почты с привязкой к владельцу домена или к регистрации, стороны, связанные договорными обязательствами, должны, как минимум, учитывать следующее:

- Адреса электронной почты физических лиц, привязанные к владельцу домена или регистрации, скорее всего являются персональными данными (то есть ни один из подходов не создает анонимные данные, как они определены в GDPR). Эти данные, вероятно, являются персональными данными как с точки зрения контролера данных, так и для третьих лиц.
- Однако, даже если такие данные считаются персональными, маскирование адресов электронной почты дает преимущества по сравнению с публикацией реальных адресов электронной почты владельцев доменов, в том числе: (i) демонстрирует принятие мер по повышению конфиденциальности/защите данных по замыслу (статья 25 GDPR); и (ii) несколько снижает риск, связанный с анализом баланса законных интересов при раскрытии маскированного адреса электронной почты третьим лицам.
- В целом, публикация адреса электронной почты с привязкой к регистрации, скорее всего, влечет за собой меньший риск, чем публикация адресов электронной почты с привязкой к владельцу домена, из-за объема информации, которую сторона может потенциально связать с субъектом данных на основе контактных адресов электронной почты, привязанных к владельцу домена.
- При публикации адресов электронной почты как с привязкой к владельцу домена, так и с привязкой к регистрации, стороны, связанные договорными обязательствами, должны принять эффективные меры по снижению доступности контактных данных для спамеров.

4 Дальнейшие действия

4.1 Дальнейшие действия

Настоящий итоговый отчет будет передан Совету GNSO для рассмотрения и утверждения. В случае принятия Советом GNSO итоговый отчет затем будет направлен в Правление ICANN для рассмотрения и, возможно, утверждения.

Глоссарий

1. Консультативный комитет

Консультативный комитет — официальный консультативный орган, состоящий из представителей интернет-сообщества, созданный для консультирования ICANN по конкретному вопросу или в конкретной области политики. Некоторые комитеты предусмотрены Уставом ICANN, другие могут создаваться по необходимости. Консультативный комитет не имеет полномочий действовать от лица ICANN, но может докладывать о своих результатах и давать рекомендации Правлению ICANN.

2. ALAC — Консультативный комитет At-Large

Консультативный комитет At-Large ICANN (ALAC) отвечает за обсуждение и предоставление рекомендаций по деятельности ICANN, затрагивающей интересы индивидуальных интернет-пользователей (сообщества At-Large). ICANN, как частная некоммерческая корпорация, отвечающая за техническое управление системой доменных имен и адресов интернета, опирается на ALAC и его вспомогательную инфраструктуру, чтобы вовлечь индивидуальных пользователей в деятельность ICANN и принять во внимание широкий круг их интересов.

3. Группа интересов коммерческих пользователей

Группа интересов коммерческих пользователей представляет интересы коммерческих пользователей интернета. Группа интересов коммерческих пользователей — одна из групп интересов, входящих в состав Группы коммерческих заинтересованных сторон (CSG), которая упоминается в статье 11.5 Устава ICANN. BC — одна из групп заинтересованных сторон и групп интересов Организации поддержки доменов общего пользования (GNSO), на которую возложена обязанность давать Правлению ICANN рекомендации по вопросам политики, относящимся к управлению системой доменных имен.

4. ccNSO — Организация поддержки национальных доменов

ccNSO является организацией поддержки, которая отвечает за выработку и передачу Правлению ICANN рекомендаций по глобальной политике в отношении национальных доменов верхнего уровня. Она выступает в качестве форума для регистратур национальных доменов верхнего уровня, где они могут встречаться и обсуждать важные проблемы на глобальном уровне. ccNSO избирает одного члена Правления.

5. ccTLD — национальный домен верхнего уровня

ccTLD — это домены, состоящие из двух букв, например .UK (Великобритания), .DE (Германия) и .JP (Япония). Они называются национальными доменами верхнего уровня (ccTLD) и соответствуют стране, территории или другому географическому местоположению. Правила и политика регистрации доменных имен в ccTLD

значительно разнятся, и регистратуры ccTLD разрешают использовать ccTLD только жителям соответствующей страны.

Дополнительную информацию о ccTLD, включая полную базу данных выделенных ccTLD и назначенных администраторов см. здесь: <http://www.iana.org/cctld/cctld.htm>.

6. Регистрационные данные доменного имени

Регистрационные данные доменного имени (их также называют регистрационными данными) — это информация, которую предоставляют при регистрации доменного имени владельцы доменов и собирают регистраторы или регистратуры. Некоторые из этих данных становятся общедоступными. Что касается взаимодействия между аккредитованными ICANN регистраторами и владельцами доменов общего пользования верхнего уровня (gTLD), элементы данных указаны в действующей редакции RAA. Для национальных доменов верхнего уровня (ccTLD) операторы этих TLD определяют политику запроса и отображения регистрационных данных самостоятельно или в соответствии с указаниями соответствующего правительства.

7. Доменное имя

В системе доменных имен доменные имена служат идентификаторами ресурсов интернет-протокола, например интернет-сайтов.

8. DNS — система доменных имен

DNS — это система доменных имен интернета. Система доменных имен (DNS) помогает пользователям ориентироваться в интернете. У каждого компьютера в интернете есть свой уникальный адрес — как номер телефона — и он состоит из довольно сложной последовательности цифр. Этот адрес называется IP-адресом (сокращение IP означает «интернет-протокол»). IP-адреса трудно запомнить. Система DNS упрощает использование интернета, позволяя вводить строку из букв (доменное имя) вместо непонятного IP-адреса. Поэтому, вместо того чтобы вводить цифры 207.151.159.3, можно ввести www.internic.net. Это мнемонический способ, облегчающий запоминание адресов.

9. EPDP — Ускоренный процесс формирования политики GNSO

Ряд формальных этапов, описанных в Уставе ICANN и направленных на инициирование разработки, внутренний и внешний анализ, составление графика выработки и одобрения политики, необходимой для координации глобальной системы уникальных идентификаторов интернета. EPDP может начаться по инициативе Совета GNSO только в следующих особых ситуациях: (1) решение узкого вопроса политики, который выявлен и определен либо после одобрения Правлением ICANN рекомендации GNSO по политике, либо во время реализации такой одобренной рекомендации; или (2) предоставление новых или дополнительных рекомендаций по конкретному вопросу политики, который практически определен ранее и по которому уже имеется обширная и уместная вспомогательная

информация, например (а) отчет о неразрешенных проблемах для возможного PDP, который не был инициирован; (б) материалы предыдущего незавершенного PDP; (в) другие проекты, такие как Методологический процесс GNSO.

10. GAC — Правительственный консультативный комитет

GAC — консультативный комитет, состоящий из назначенных представителей национальных правительств, многонациональных правительственных организаций и организаций договора, а также обособленных экономических регионов. Его функция заключается в консультировании Правления ICANN по вопросам, относящимся к деятельности правительств. GAC служит форумом для обсуждения правительственных интересов и проблем, включая интересы потребителей. Как и любой другой консультативный комитет, GAC не уполномочен действовать от лица ICANN, но может докладывать о своих выводах и давать рекомендации Правлению ICANN.

11. Общие положения о защите данных (GDPR)

Общие положения о защите данных (ЕС) 2016/679 (GDPR) — нормативный акт ЕС о защите данных и конфиденциальности всех граждан Европейского Союза (ЕС) и Европейской экономической зоны (ЕЭЗ). В нем также рассматриваются вопросы экспорта персональных данных за пределы ЕС и ЕЭЗ.

12. GNSO — Организация поддержки доменов общего пользования

Организация поддержки, которая отвечает за разработку и передачу Правлению ICANN рекомендаций по существенным принципам политики в отношении доменов общего пользования верхнего уровня. В его состав входят представители регистратур gTLD, регистраторов gTLD, сторон, интересующихся вопросами интеллектуальной собственности, интернет-провайдеров, коммерческих и некоммерческих сторон.

13. Домен общего пользования верхнего уровня (gTLD)

gTLD — это домен верхнего уровня в DNS, делегированный корпорацией ICANN согласно имеющему полную юридическую силу соглашению об администрировании домена верхнего уровня, не являющийся национальным TLD (ccTLD) или интернационализированным доменным именем (IDN-доменом) национального TLD.

14. Группа заинтересованных сторон-регистратур gTLD (RySG)

Группа заинтересованных сторон-регистратур gTLD (RySG) является признанной организацией в составе Организации поддержки доменов общего пользования (GNSO), созданной в соответствии с разделом 5 статьи X (сентябрь 2009 года) Устава Интернет-корпорации по присвоению имен и номеров (ICANN).

Основная функция RySG — представлять интересы операторов регистратур gTLD (или спонсоров в случае спонсируемых gTLD) («Регистратуры»), которые (i) заключили договор с ICANN об оказании услуг регистратуры gTLD для обеспечения работы одного или нескольких gTLD; (ii) согласились в этом договоре соблюдать

согласованную политику; iii) решили стать членами RySG. RySG может включать группы интересов в соответствии со статьей IV. Группа RySG доводит мнения RySG до сведения Совета GNSO и Правления ICANN, уделяя особое внимание согласованной политике ICANN, относящейся к функциональной совместимости, технической надежности и (или) стабильному функционированию интернета или системы доменных имен.

15. ICANN — Интернет-корпорация по присвоению имен и номеров

Интернет-корпорация по присвоению имен и номеров (ICANN) — международная некоммерческая корпорация, которая несет ответственность за распределение адресного пространства интернет-протокола (IP-адресов), назначение идентификаторов протокола, управление системой доменных имен доменов общего пользования верхнего уровня (gTLD) и национальных доменов верхнего уровня (ccTLD), а также за функции управления системой корневых серверов. Первоначально ответственность за оказание данных услуг несли Администрация адресного пространства интернета (IANA) и другие организации согласно контракту с правительством США. Сейчас функции IANA выполняет ICANN. Корпорация занимается защитой операционной стабильности интернета, продвижением конкуренции, обеспечением широкого представительства глобальных сообществ интернета и разработкой политики, соответствующей ее миссии посредством процесса, осуществляемого по принципу «снизу-вверх» и на основании консенсуса.

16. Группа интересов по вопросам интеллектуальной собственности (IPC)

Группа интересов по вопросам интеллектуальной собственности (IPC) представляет в ICANN мнения и интересы всемирного сообщества, занимающегося вопросами интеллектуальной собственности, уделяя особое внимание защите товарных знаков, авторского права и соответствующих прав на интеллектуальную собственность, а также вопросам их влияния на систему доменных имен (DNS) и взаимодействия с этой системой. IPC — одна из групп интересов Организации поддержки доменов общего пользования (GNSO), на которую возложена обязанность давать Правлению ICANN рекомендации по вопросам политики, относящимся к управлению системой доменных имен.

17. Группа интересов интернет-провайдеров и провайдеров связи (ISPCP)

Группа интересов интернет-провайдеров и провайдеров связи (ISPCP) — это группа интересов, входящая в состав GNSO. Цель этой группы интересов — выполнение функций и обязанностей, которые зафиксированы в соответствующих положениях уставов ICANN и GNSO, соблюдение политики или правил, которые корпорация ICANN принимает в результате своей деятельности. ISPCP обеспечивает, чтобы мнения интернет-провайдеров и провайдеров связи вносили вклад в достижение целей и выполнение задач ICANN.

18. DNS-сервер

DNS-сервер — это компонент системы доменных имен, который хранит информацию об одной зоне (или нескольких зонах) пространства имен DNS.

19. Группа некоммерческих заинтересованных сторон (NCSG)

Группа некоммерческих заинтересованных сторон (NCSG) — это группа заинтересованных сторон, входящая в состав GNSO. Цель Группы некоммерческих заинтересованных сторон (NCSG) — представлять через избранных представителей и свои группы интересов проблемы и интересы владельцев доменов и интернет-пользователей доменов общего пользования верхнего уровня gTLD, не занимающихся коммерческой деятельностью. Она дает возможность высказать свое мнение и направить представителей для участия в процессах ICANN следующим лицам: некоммерческие организации, которые служат некоммерческим интересам или оказывают услуги некоммерческого характера в сфере образования, благотворительности, защиты потребителей, создания местных общественных организаций, поддержки искусства, защиты принципов общественной политики, благополучия детей, религии, научных исследований и прав человека; некоммерческие организации, которые отстаивают общественные интересы в области разработки программного обеспечения; семьи или физические лица, которые регистрируют доменные имена для личного некоммерческого использования; интернет-пользователи, которые проявляют особый интерес к некоммерческим аспектам политики в отношении доменных имен, имеющим отношение к общественным интересам.

20. Процедуры разрешения разногласий после делегирования (PDDRP)

Процедуры разрешения разногласий после делегирования были разработаны, чтобы у сторон, пострадавших в результате действий оператора регистратуры нового gTLD, была альтернативная возможность подачи жалобы на такие действия. Такие процедуры разрешения разногласий проводятся внешними поставщиками, независимыми от ICANN, и могут потребовать, чтобы истец предпринял конкретные шаги по решению своих проблем до подачи официальной жалобы. Экспертная комиссия определяет, совершил ли оператор регистратуры нарушение, и рекомендует ICANN меры по исправлению ситуации.

21. Зарегистрированное имя

«Зарегистрированное имя» означает доменное имя в gTLD, состоящее из двух (2) или более (например, john.smith.name) уровней, о котором оператор регистратуры gTLD (или его аффилированная организация или подрядчик, участвующий в оказании услуг регистратуры) хранит данные в базе данных регистратуры, организует такое хранение или получает доходы от такого хранения. Имя в базе данных регистратуры может быть зарегистрированным именем, даже если оно не внесено в файл зоны (например, зарегистрированное, но неактивное доменное имя).

22. Регистратор

Слово «регистратор», начинающееся со строчной буквы, означает физическое или юридическое лицо, которое вступает в договорные отношения с владельцами зарегистрированных имен и оператором регистратуры, собирает регистрационные данные владельцев зарегистрированных имен и передает регистрационную информацию для занесения в базу данных регистратуры.

23. Группа заинтересованных сторон-регистраторов (RrSG)

Группа заинтересованных сторон-регистраторов — это одна из нескольких групп заинтересованных сторон сообщества ICANN, которая является представительным органом регистраторов. Это разнообразная и активная группа, работа которой направлена на эффективную защиту интересов регистраторов и их клиентов. Мы предлагаем вам подробнее узнать об аккредитованных регистраторах доменных имен и важных функциях, которые они выполняют в системе доменных имен.

24. Оператор регистратуры

«Оператор регистратуры» — это физическое или юридическое лицо, которое отвечает за оказание услуг регистратуры для конкретного gTLD в соответствии с соглашением между ICANN (или ее правопреемником) и этим физическим или юридическим лицом (этими физическими или юридическими лицами) или, если такое соглашение расторгнуто или его срок действия завершился, в соответствии с соглашением между правительством США и этим физическим или юридическим лицом (этими физическими или юридическими лицами).

25. Служба каталогов регистрационных данных (RDDS)

Служба каталогов регистрационных данных доменных имен или RDDS — это служба, предлагаемая (службы, предлагаемые) регистратурами и регистраторами для доступа к регистрационным данным доменных имен.

26. Процедура разрешения споров по ограничениям регистрации (RRDRP)

Процедура разрешения споров по ограничениям регистрации (RRDRP) предназначена для использования в ситуациях, когда оператор регистратуры нового gTLD от сообщества не соблюдает ограничения регистрации, изложенные в его Соглашении об администрировании домена верхнего уровня.

27. SO — организации поддержки

SO — это три специальных консультативных органа, которые дают Правлению ICANN рекомендации по вопросам, касающимся доменных имен (GNSO и CCNSO) и IP-адресов (ASO).

28. SSAC — Консультативный комитет по безопасности и стабильности

Консультативный комитет Правления ICANN, в состав которого входят технические эксперты из отрасли и сектора науки и образования, а также операторы корневых серверов интернета, регистраторы и регистратуры TLD.

29. TLD — домен верхнего уровня

TLD — это имена верхнего уровня в иерархии имен DNS. Они отображаются в доменных именах как набор символов за последней (крайней справа) точкой, например «net» в <http://www.example.net>. Администратор TLD контролирует, какие доменные имена второго уровня распознаются в этом TLD. Администратор «корневого домена» или «корневой зоны» контролирует, какие TLD распознаются системой DNS. К широко используемым TLD относятся .COM, .NET, .EDU, .JP, .DE и так далее.

30. Единая политика разрешения споров о доменных именах (UDRP)

Единая политика разрешения споров о доменных именах (UDRP) — это механизм защиты прав, который устанавливает процедуры и правила, применяемые регистраторами при возникновении споров в связи с регистрацией и использованием доменных имен в gTLD. UDRP обеспечивает наличие малозатратной административной процедуры, в результате которой принимаются обязательные для исполнения решения, предназначенной для урегулирования претензий в связи со злонамеренной, недобросовестной регистрацией доменных имен. Она применяется только к спорам между владельцами доменов и третьими сторонами, но не к спорам между регистратором и его клиентом.

31. Служба быстрой приостановки (URS)

Служба быстрой приостановки — это механизм защиты прав, который дополняет существующую Единую политику разрешения споров о доменных именах (UDRP), предоставляя правообладателям, столкнувшимся с наиболее очевидными случаями нарушения своих прав, менее дорогостоящий и более быстрый способ решения проблемы.

32. WHOIS

Протокол WHOIS — это протокол интернета, который используется для отправки запросов к базам данных с целью получения регистрационных данных доменного имени (или IP-адреса). Первоначально протокол WHOIS был определен в документе RFC 954, опубликованном в 1985 году. Документом действующей спецификации является RFC 3912. Соглашения ICANN с gTLD требуют, чтобы регистратуры и регистраторы предлагали интерактивную веб-страницу и услугу WHOIS через порт 43 с бесплатным открытым доступом к сведениям о зарегистрированных именах. Эти сведения обычно называются «данными WHOIS» и включают такие элементы, как дата регистрации и дата окончания срока регистрации доменного имени, DNS-серверы, контактные данные владельца домена и назначенных контактных лиц по административным и техническим вопросам.

Службы WHOIS в основном используются для идентификации личности владельцев доменов в бизнес-целях и для определения сторон, способных устранить проблемы, связанные с зарегистрированным доменом.

Приложение А. Историческая справка

По просьбе некоторых участников группы по EPDP Совет GNSO предложил группе по EPDP после завершения фаз 1 и 2 продолжить работу над двумя темами, а именно: 1) дифференциация регистрационных данных юридических и физических лиц и 2) возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов.

Дифференциация данных юридических и физических лиц — поручения Совета группе по EPDP

Что касается дифференциации юридических и физических лиц, ожидается, что группа по EPDP рассмотрит [результаты предпринятого корпорацией ICANN исследования](#) (выполненного по запросу группы по EPDP и одобренного Советом GNSO во время Фазы 1) наряду с [юридическими рекомендациями](#) компании Bird & Bird, а также предложениями по существу данного вопроса, поступившими в ходе [форума общественного обсуждения дополнения](#), и ответит на следующие вопросы:

- i. Необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»);
- ii. Необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие.

Возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов — поручения Совета группе по EPDP

Ожидается, что группа по EPDP проанализирует [юридические рекомендации](#) и рассмотрит конкретные предложения в отношении достаточных мер защиты, призванных устранить проблемы, отмеченные в докладной записке по юридическим вопросам. На группы, которые попросили выделить им дополнительное время на рассмотрение этой темы (ALAC GAC и SSAC), возлагается ответственность за выработку соответствующих конкретных предложений. В итоге предполагается получить ответы на следующие вопросы:

- i. Имеется ли возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, и если да, должно ли это стать требованием.
- ii. Если это осуществимо, но не является требованием, какие указания следует дать связанным договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты.

Приложение В. Общие сведения

История процесса и вопроса

19 июля 2018 года Совет GNSO [инициировал](#) Ускоренный процесс формирования политики (EPDP) и [учредил](#) группу по EPDP в области Временной спецификации для регистрационных данных в gTLD. В отличие от других PDP GNSO, в которых может участвовать любой, Совет GNSO решил ограничить членский состав группы по EPDP, главным образом, исходя из необходимости выполнить работу в сравнительно короткий срок и ответственно подойти к выделению ресурсов на эту деятельность. Группам заинтересованных сторон GNSO, Правительственному консультативному комитету (GAC), Организации поддержки национальных доменов (ccNSO), Консультативному комитету At-Large (ALAC), Консультативному комитету системы корневых серверов (RSSAC) и Консультативному комитету по безопасности и стабильности (SSAC) было предложено назначить определенное количество членов и их дублеров, как указано в [уставе](#). Кроме того, Правлению и корпорации ICANN было предложено назначить несколько представителей в состав этой группы. Для формирования вышеупомянутых групп в июле было опубликовано объявление о наборе волонтеров, и [1 августа 2018 года](#) группа по EPDP провела свое первое совещание в рамках Фазы 1.

История вопроса

17 мая 2018 года Правление ICANN приняло Временную спецификацию для регистрационных данных в gTLD. Правление сделало это, чтобы установить для ICANN и сторон, связанных договорными обязательствами, временные условия соблюдения действующих контрактных требований и выработанной сообществом политики в области WHOIS и одновременно обеспечить соблюдение Общих положений о защите данных (GDPR) Европейского Союза (ЕС). Временная спецификация была принята согласно процедуре подготовки временных спецификаций, определенной Соглашением об администрировании домена верхнего уровня (RA) и Соглашением об аккредитации регистраторов (RAA). После утверждения Временной спецификации Правление «должно незамедлительно начать процесс разработки согласованной политики, который определен в Уставе ICANN»⁴⁸. Процесс разработки согласованной политики в области Временной спецификации должен быть выполнен за один год. Кроме того, одной из его задач является обсуждение системы стандартизованного доступа к закрытым регистрационным данным.

⁴⁸ См. раздел 3.1(a) Соглашения об администрировании домена верхнего уровня:
<https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en>

На заседании 19 июля 2018 года Совет Организации поддержки доменов общего пользования (GNSO) запустил EPDP в области Временной спецификации для регистрационных данных в gTLD и принял устав группы по EPDP. В отличие от других PDP GNSO, в которых может участвовать любой, Совет GNSO решил ограничить членский состав группы по EPDP, главным образом, исходя из необходимости выполнить работу в сравнительно короткий срок и ответственно подойти к выделению ресурсов на эту деятельность. Группам заинтересованных сторон GNSO, Правительственному консультативному комитету (GAC), Организации поддержки национальных доменов (ccNSO), Консультативному комитету At-Large (ALAC), Консультативному комитету системы корневых серверов (RSSAC) и Консультативному комитету по безопасности и стабильности (SSAC) было предложено назначить определенное количество членов и их дублеров, как указано в [уставе](#). Кроме того, Правлению и корпорации ICANN было предложено назначить несколько представителей в состав этой группы.

Совет GNSO проголосовал за принятие всех 29 рекомендаций [итогового отчета](#) по Фазе 1 EPDP на своем заседании 4 марта 2019 года. 15 мая 2019 года Правление ICANN [приняло](#) окончательный отчет по итогам работы группы по EPDP над Фазой 1, за исключением отдельных частей двух рекомендаций: 1) Цель № 2 в рекомендации № 1 и 2) возможность удаления данных в поле «Организация» в рекомендации № 12. В соответствии с Уставом ICANN между Советом GNSO и Правлением ICANN были проведены консультации для обсуждения тех частей рекомендаций Фазы 1 EPDP, которые не были приняты Правлением ICANN. В то же время Группа по проверке выполнения рекомендаций (IRT), состоящая из представителей корпорации ICANN и членов сообщества ICANN, теперь работает над выполнением утвержденных рекомендаций окончательного отчета по итогам работы группы по EPDP над Фазой 1. Дополнительные сведения о статусе реализации см. [здесь](#).

Совет GNSO утвердил [итоговый отчет по Фазе 2](#) на заседании 24 сентября 2020 года суперквалифицированным большинством. В отчет вошли рекомендации группы по EPDP относительно Системы обеспечения стандартизованного доступа к закрытым регистрационным данным gTLD и их раскрытия (SSAD) и рекомендации и выводы относительно так называемых вопросов второго уровня приоритетности, к которым относятся, в том числе, хранение данных и вымарывание поля «Город».

В рамках своего одобрения Совет GNSO согласился запросить консультацию с Правлением ICANN для обсуждения финансовой устойчивости SSAD и некоторых проблем, выраженных в различных заявлениях меньшинства, включая вопрос о том, следует ли провести дополнительный анализ затрат и выгод до того, как Правление ICANN рассмотрит все связанные с SSAD рекомендации для принятия. В ходе ICANN70 Правление поручило корпорации ICANN начать фазу функциональной разработки (ODP) для рекомендаций, связанных с SSAD, и в настоящее время эта ODP продолжается. Подробнее об ODP SSAD см. [здесь](#).

Поскольку запрошенная консультация касалась только рекомендаций, связанных с SSAD, Правление решило рассмотреть рекомендации, имеющие второй уровень приоритетности, отдельно и провело период [общественного обсуждения](#) этих рекомендаций с декабря 2020 года по январь 2021 года. С февраля по март 2021 года Правление провело отдельный период [общественного обсуждения](#) рекомендаций, касающихся SSAD.

По просьбе некоторых участников группы по EPDP Совет GNSO предложил группе по EPDP продолжить работу над двумя темами в рамках фазы 2А, а именно: 1) дифференциация регистрационных данных юридических и физических лиц и 2) возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов.

Приложение С. Состав группы по EPDP и участие в заседаниях

Состав группы по EPDP и участие в заседаниях

Сводка по работе на заседаниях:

Пленарные заседания:

- 42 пленарные телеконференции (5 отменено) общей продолжительностью 53,5 ч, всего 1924,5 человеко-часов
- Суммарная доля участия 85,3%

Заседания Юридического комитета:

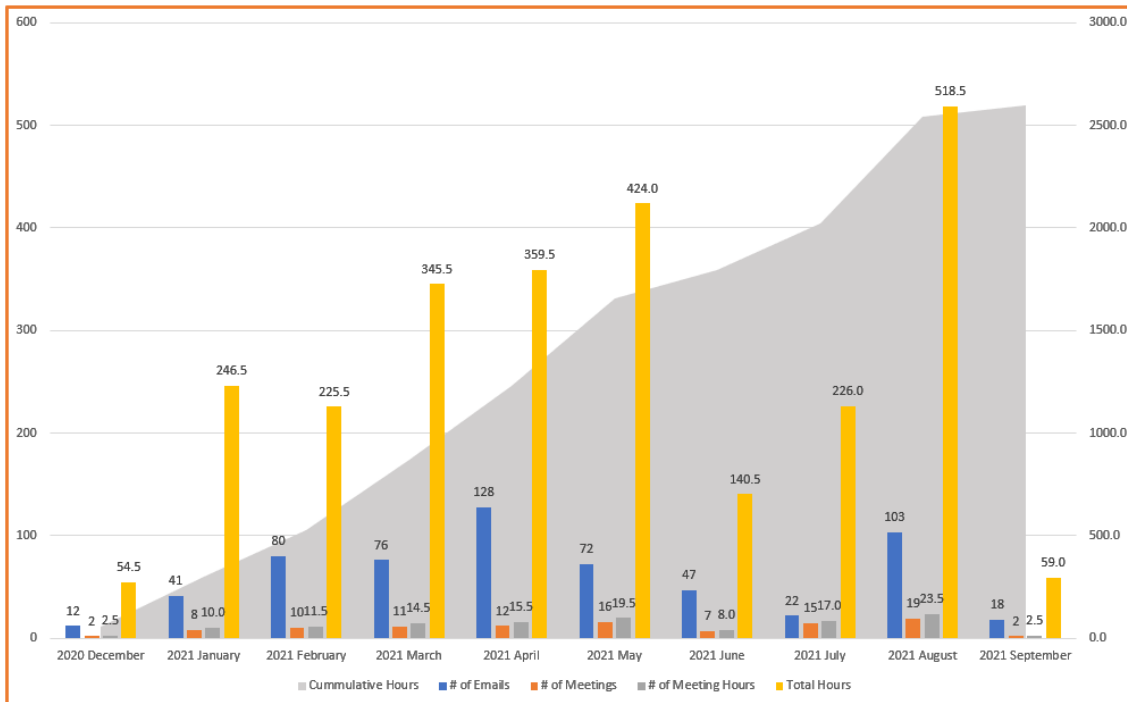
- 11 телеконференций в подгруппах общей продолжительностью 17,5 ч, всего 232,5 человеко-часов
- Суммарная доля участия 89,2%

Заседания малых групп:

- 16 телеконференций в подгруппах общей продолжительностью 17,5 ч, всего 180,0 человеко-часов
- Суммарная доля участия 99,0%

Заседания руководства:

- 51 телеконференций руководства общей продолжительностью 39,0 ч, всего 268,5 человеко-часов



Архивы электронной почты группы по EPDP находятся здесь:
<https://mm.icann.org/pipermail/gnso-epdp-team/>.

Участники группы по EPDP:

Представленная группа/участник	SOI	Дата начала	Дата ухода	Участие в совещаниях, %	Роль
Консультативный комитет At-Large (ALAC)				98,6%	
Алан Гринберг (Alan Greenberg)	SOI	15 ноября 2020 года		97,2%	
Хадия Эльминьяви (Hadia Elminiawi)	SOI	15 ноября 2020 года		100,0%	LC
Группа интересов коммерческих пользователей (BC)				88,9%	
Марджи Милам (Margie Milam)	SOI	15 ноября 2020 года		86,1%	LC
Марк Сванкарек (Mark Svancarek)	SOI	15 ноября 2020 года		91,7%	
Совет GNSSO				88,7%	
Брайан Бекхэм (Brian Beckham)	SOI	18 февраля 2021 года		86,2%	Заместитель председателя, LC
Кит Дрейзек (Keith Drazek)	SOI	12 марта 2020 года		97,2%	Председатель, LC
Филипп Фукар (Philippe Fouquart)	SOI	26 января 2021 года		81,3%	Представитель, LC
Правительственный консультативный комитет (GAC)				74,1%	
Кристофер Льюис-Эванс (Christopher Lewis-Evans)	SOI	19 ноября 2020 года		88,9%	
Лорин Капин (Laureen Kapin)	SOI	19 ноября 2020 года		83,3%	LC
Мелина Струнги (Melina Stroungi)	SOI	20 ноября 2020 года		50,0%	LC
Правление ICANN				73,6%	
Бекки Берр (Becky Burr)	SOI	12 ноября 2020 года		75,0%	Представитель, LC
Мэтью Ширс (Matthew Shears)	SOI	12 ноября 2020 года		72,2%	Представитель
Группа интересов по вопросам интеллектуальной собственности (IPC)				84,7%	
Брайан Кинг (Brian King)	SOI	20 ноября 2020 года		97,2%	LC
Ян Янсен (Jan Janssen)	SOI	20 ноября 2020 года		72,2%	LC
Интернет-корпорации по присвоению имен и номеров (ICANN)				93,1%	
Эми Бивинс (Amy Bivins)	SOI	12 июля 2020 года		88,9%	Представитель, LC
Брайан Гуттерман (Brian Gutterman)	SOI	12 октября 2020 года		97,2%	Представитель
Группа интересов интернет-провайдеров и провайдеров связи (ISPCP)				93,1%	
Кристиан Доусон (Christian Dawson)	SOI	15 ноября 2020 года		94,4%	
Томас Рикерт (Thomas Rickert)	SOI	15 ноября 2020 года		91,7%	LC
Группа некоммерческих заинтересованных сторон (NCSG)				65,0%	
Дэвид Кейк (David Cake)	SOI	12 марта 2020 года		72,2%	
Манджу Чен (Manju Chen)	SOI	12 марта 2020 года		97,2%	

Милтон Мюллер (Milton Mueller)	SOI	12 марта 2020 года		58,3%	
Стефан Филипович (Stefan Filipovic)	SOI	12 марта 2020 года		13,9%	LC
Стефани Перрин (Stephanie Perrin)	SOI	12 марта 2020 года		83,3%	LC
<Вакантно>					
Группа заинтересованных сторон-регистраторов (RrSG)				70,4%	
Джеймс Блейдел (James Bladel)	SOI	15 ноября 2020 года		27,8%	
Сара Уайлд (Sarah Wyld)	SOI	15 ноября 2020 года		94,4%	
Волкер Грейман (Volker Greimann)	SOI	15 ноября 2020 года		88,9%	LC
Группа заинтересованных сторон-регистратор (RySG)				94,4%	
Алан Вудс (Alan Woods)	SOI	15 ноября 2020 года		91,7%	LC
Марк Андерсон (Marc Anderson)	SOI	15 ноября 2020 года		97,2%	
Мэтью Кроссмэн (Matthew Crossman)	SOI	15 ноября 2020 года		94,4%	LC
Консультативный комитет по безопасности и стабильности (SSAC)				98,5%	
Бен Батлер (Ben Butler)	SOI	15 ноября 2020 года	14 января 2021 года	50,0%	
Стив Крокер (Steve Crocker)	SOI	2 октября 2021 года		100,0%	
Тара Уэйлен (Tara Whalen)	SOI	15 ноября 2020 года		100,0%	LC

LC = работал в Юридическом комитете

Дублерами членов группы по EPDP являются следующие лица:

Представленная группа/Дублер	SOI	Дата начала	Дата ухода	Участие в совещаниях, %	Роль
Консультативный комитет At-Large (ALAC)					
Холли Рэйчи (Holly Raiche)	SOI	15 ноября 2020 года		100,0%	
<Вакантно>					
Группа интересов коммерческих пользователей (BC)					
Стив Дельбьянко (Steve DelBianco)	SOI	15 ноября 2020 года		93,3%	
Правительственный консультативный комитет (GAC)					
Райан Кэрролл (Ryan Carroll)	SOI	26 января 2021 года		100,0%	
Велимира Немигенчева-Грау (Velimira Nemiguentcheva-Grau)	SOI	26 января 2021 года		100,0%	
<Вакантно>					
Правление ICANN					
Леон Фелипе Санчес Амбиа (León Felipe Sánchez Ambía)	SOI	12 ноября 2020 года		86,7%	
Группа интересов по вопросам интеллектуальной собственности (IPC)					
<Вакантно>					

Группа интересов интернет-провайдеров и провайдеров связи (ISPCP)					
Суман Лал Прадхан (Suman Lal Pradhan)	SOI	15 ноября 2020 года		100,0%	
Группа некоммерческих заинтересованных сторон (NCSG)					
Бруна Сантос (Bruna Santos)	SOI	12 марта 2020 года		100,0%	
<Вакантно>					
<Вакантно>					
Группа заинтересованных сторон-регистраторов (RrSG)					
Мэтт Серлин (Matt Serlin)	SOI	15 ноября 2020 года		100,0%	
Оуэн Смигельски (Owen Smigelski)	SOI	15 ноября 2020 года		97,0%	
Тео Гертс (Theo Geurts)	SOI	15 ноября 2020 года		100,0%	
Группа заинтересованных сторон-регистратур (RySG)					
Амр Элсадр (Amr Elsadr)	SOI	15 ноября 2020 года		100,0%	
Бет Бейкон (Beth Bacon)	SOI	15 ноября 2020 года		100,0%	
Шон Басери (Sean Baseri)	SOI	15 ноября 2020 года		100,0%	
Консультативный комитет по безопасности и стабильности (SSAC)					
Грег Аарон (Greg Aaron)	SOI	15 ноября 2020 года		100,0%	
<Вакантно>					

Персонал поддержки группы по EPDP:

Представленная группа/ прикомандированный сотрудник	SOI	Дата начала	Дата ухода	Участие в совещаниях, %	Роль
Андреа Гландон (Andrea Glandon)		15 ноября 2020 года			
Берри Кобб (Berry Cobb)		15 ноября 2020 года			
Кейтлин Туберген (Kaitlin Tubergen)		15 ноября 2020 года			LC
Джули Бисланд (Julie Bisland)		15 ноября 2020 года			
Марика Конингс (Marika Konings)		15 ноября 2020 года			
Терри Эгню (Terri Agnew)		15 ноября 2020 года			

Приложение D. Заявления меньшинства

[Комитет At-Large](#)

[Группа интересов коммерческих пользователей](#)

[Группа интересов по вопросам интеллектуальной собственности](#)

[Правительственный консультативный комитет](#)

[Группа некоммерческих заинтересованных сторон](#)

[Группа заинтересованных сторон-регистраторов](#)

[Группа заинтересованных сторон-регистратур](#)

[Консультативный комитет по безопасности и стабильности](#)

КОНСУЛЬТАТИВНЫЙ КОМИТЕТ AT-LARGE
Окончательный отчет по итогам работы над Фазой 2А ускоренного процесса
формирования политики по Временной спецификации для
регистрационных данных в gTLD

Заявление меньшинства ALAC

ALAC одобряет и высоко оценивает работу группы по EPDP над Фазой 2А, деятельность председателя, заместителя председателя и представителя в Совете GNSO, а также целеустремленность и усилия персонала поддержки из корпорации ICANN. Тем не менее, ALAC считает, что на Фазе 2А группа не реализовала должным образом свой мандат. В итоге важность регистрационных данных для различных членов сообщества, таких как агентства по защите прав потребителей, правоохранительные органы и следователи по кибербезопасности, а также решающая роль, которую они играют в защите обычных интернет-пользователей, владельцев доменов, клиентов, предприятий и всех, кто имеет отношение к интернету, не учтена должным образом.

Важно найти баланс между защитой персональной информации владельцев доменов и удобством работы, безопасностью и защищенностью пользователей. Вымарывание данных, которые не защищены законами о защите информации, не позволяет достичь правильного баланса.

В данном заявлении меньшинства ALAC выражает обеспокоенность следующими аспектами рекомендаций итогового отчета по Фазе 2А и их влиянием на безопасность и защищенность обычных интернет-пользователей:

- Отсутствие обязательного разграничения данных юридических и физических лиц
- Отсутствие требования об использовании общего элемента данных всеми сторонами, связанными договорными обязательствами
- Отсутствие средств для связи с владельцами доменов
- «Процесс»

Отсутствие обязательного разграничения данных юридических и физических лиц

GDPR не защищает данные юридических лиц, которые не относятся к персональным. Более того, в преамбуле 14 GDPR ЕС сказано, что «этот регламент не распространяется на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица».

EPDP получила юридические рекомендации о том, что целесообразно разрешить владельцам доменов самостоятельно указывать свой статус, а при наличии надлежащих предостережений, отказов от ответственности и возможностей внесения исправлений, риск для сторон, связанных договорными обязательствами,

невелик. Эта позиция была поддержана в письме EDPB, направленном Йорану Марби в июле 2018 года. Группа по EPDP проигнорировала эту рекомендацию. Хотя для обработки созданной базы в 200 млн регистраций потребуется некоторое время (например, при продлении), группа по EPDP не порекомендовала даже дифференциацию новых регистраций. Более того, даже предложение обсудить возможность принятия таких мер (официально выдвинутое членами группы по EPDP из GAC) было попросту отклонено на начальной стадии Фазы 2А, и вместо этого группа сосредоточилась только на «указаниях», которые можно проигнорировать. Принимая во внимание все вышесказанное, наряду с тем, что Служба каталогов регистрационных данных (RDDS) является общественным благом, которое защищает онлайн-пользователей по всему миру, а GDPR и аналогичные законы о конфиденциальности являются общественным благом, которое защищает регистрационные данные владельцев доменов, необходимо найти правильный баланс. Этот правильный баланс невозможно достигнуть, если вымарывать больше данных, чем требуется по законодательству, и группа по EPDP практически не приложила усилий для достижения этого баланса.

Отсутствие требования об использовании общего элемента данных всеми сторонами, связанными договорными обязательствами

Предлагаемый в Рекомендации № 1 общий элемент (элементы) данных допускает восемь возможных значений, в том числе «разграничение по правовому статусу не проводилось» и «наличие персональных данных не определялось». Эти состояния позволяют сторонам, связанным договорными обязательствами, которые не проводят различий, использовать созданное новое поле. Однако группа по EPDP не рекомендовала обязательное использование этих полей даже теми регистраторами, которые добровольно решили дифференцировать юридических и физических лиц или указывать на наличие/отсутствие персональных данных. Нелепо отказываться от введения требования об использовании этих полей ДАЖЕ ТОГДА, КОГДА имеются достоверных и полезных данных. Более того, группа по EPDP не обозначила эти поля как подлежащие публичному раскрытию, хотя они НЕ содержат персональной информации.

Согласно рекомендациям окончательных отчетов по итогам фаз 1 и 2 EPDP, стороны, связанные договорными обязательствами (CP), должны обновить свои текущие службы каталогов регистрационных данных (RDDS).

Обязательное использование общего элемента данных всеми сторонами, связанными договорными обязательствами, позволит всем CP по всему миру соблюдать одинаковые процессы, независимо от того, проводят ли они разграничение данных и подпадают ли они под действие нормативных актов ЕС.

В результате мы создаем общий элемент, который никто не обязан использовать, что сводит на нет попытку создания единых подходов к работе и открывает путь к разрозненности.

Отсутствие средств для связи с владельцами доменов

ALAC сожалеет, что группе по EPDP не удалось завершить работу над методами, позволяющими более эффективно решить проблему анонимизации или псевдонимизации контактных адресов электронной почты. При этом мы остаемся с рекомендациями Фазы 1, допускающими анонимизацию, однако в силу отсутствия этих методов, разрешаем использовать веб-формы для контактов. После завершения Фазы 1 стало очевидно, что некоторые (крупные) регистраторы используют такие веб-формы такого вида, который фактически не обеспечивает возможность полезных контактов с владельцем домена. Устранение этого очевидного пробела в правилах было признано не входящим в круг задач группы, несмотря на указания GNSO вернуться к рассмотрению этой рекомендации Фазы 1. Конечный результат состоит в том, что для значительной части регистрационной базы gTLD нет эффективного способа связи с владельцами доменов.

«Процесс»

ALAC обеспокоен тем, что на протяжении всего EPDP основное внимание уделяется исключительно намеченным процессам и заявленным срокам, что серьезно влияет на способность сформировать и рекомендовать качественную политику.

Вот несколько примеров:

- Сроки, которые не позволяют провести достаточное количество дискуссий и консультаций с группами, поддерживающими данный EPDP.
- Установленный круг задач, из которого был исключен ряд пунктов, поскольку они прямо не упомянуты в поручениях GNSO, но при этом были допущены другие отклонения (например, рекомендация по Кодексу поведения).
- Приостановка обсуждения дифференциации в пользу «указаний», с невыполненным обещанием вернуться к этому вопросу.
- Непоследовательные стандарты «доказательств», которые позволяют отвергать одни аргументы, в то время как другие остаются в силе.

Судя по всему, стороны, связанные договорными обязательствами, все чаще отказываются брать на себя ЛЮБЫЕ новые обязательства, независимо от выгоды для других сторон или общественного блага. Эта тенденция вызывает беспокойство.

Резюме

В время Фазы 1 EPDP было принято решение «изучить и урегулировать вопрос о проведении различий между физическими и юридическими лицами» на Фазе 2. Этот вопрос был отложен до Фазы 2А. Очевидно, что мы его не решили. Более того, хотя мы рекомендовали создать важнейшие элементы RDDS, мы позволяем полностью игнорировать их. ALAC с большим трудом может назвать эту работу успешной.

**Заявление меньшинства Группы интересов коммерческих пользователей
касательно окончательного отчета по итогам работы группы по
EPDP над Фазой 2А⁴⁹
10 сентября 2021 года**

Введение

Настоящее заявление меньшинства представлено от имени Группы интересов коммерческих пользователей ICANN (BC)⁵⁰.

BC является ярким сторонником прав на неприкосновенность частной жизни и регламента GDPR, который предназначен для их защиты. Однако в контексте работы группы по EPDP над этим ускоренным процессом формирования политики (EPDP) — группы, которой было прямо поручено «сохранить базу данных WHOIS в максимально возможной степени», соблюдая при этом законы о защите конфиденциальной информации — итоговая политика превышает то, что необходимо для защиты данных физических лиц.

Совет GNSO поручил группе по EPDP на Фазе 2А сосредоточиться на двух конкретных темах: 1) дифференциация регистрационных данных юридических и физических лиц и 2) возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов. Наш комментарий сосредоточен на разграничении данных юридических и физических лиц, на отсутствии достижимых в принудительном порядке результатов и, что важно, на настоятельной потребности отреагировать на европейский законодательный прогресс, который повлияет на разработанную политику, или на отсутствие таковой.

Как уже говорилось ранее, BC твердо убеждена, что необязательное разграничение данных юридических и физических лиц является недостаточной мерой и что политика ICANN должна сделать такое разграничение обязательным для обеспечения безопасности и стабильности глобальной DNS.

В целом, рекомендации Фазы 2А, не проводя различий между юридическими и физическими лицами, приводят к тому, что значительное количество регистрационных записей будет вымарано или недоступно по другим причинам. Это огорчает и даже разочаровывает, учитывая известную распространенность вреда, наносимого в интернете. Такое разочарование хорошо задокументировано

⁴⁹ 3 сентября 2021 года, окончательный отчет по итогам работы группы по EPDP над Фазой 2А: <https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20210903/4c231c0a/EPDPPhase2A-FINALREPORT-3September2021003-0001.pdf>

⁵⁰ Предыдущие комментарии BC и заявление меньшинства по Фазе 2 EPDP:

- BC и IPC представили [совместное заявление меньшинства по Фазе 2 EPDP](#).
- [Комментарии BC к первоначальному отчету по Фазе 2А](#)

в недавнем исследовании Рабочей группы по борьбе со злоупотреблением рассылкой сообщений (М3ААWG)⁵¹, которая подробно описала существенные ограничения текущего доступа к закрытым регистрационным записям доменных имен и подтвердила, что решения, обсуждаемые в настоящее время ICANN, не позволят удовлетворить потребности правоохранительных органов и специалистов по кибербезопасности.

Хотя группа по EPDP обозначила свои рекомендации как поддержанные «консенсусом», ВС вновь заявляет, что не поддерживает результаты Фазы 2А, не поддерживает обозначение «консенсус» и в настоящем документе приводит обоснование своего несогласия.

Мнение ВС об окончательном отчете по итогам работы группы по EPDP над Фазой 2А

Основным принципом выполнения миссии ICANN является формирование согласованной политики, способствующей безопасности и стабильности DNS, и неукоснительное соблюдение всех обязательств, вытекающих из такой политики. Однако ВС отмечает появившуюся недавно тенденцию — особенно ярко выраженную в обсуждениях и результатах Рабочей группы (РГ) Фазы 2А — опираться на «факультативные» обязательства (например, использование слов «следует» и «может» в формулировках рекомендаций), что является уклонением от обязательств и свидетельствует об отсутствии твердой приверженности сохранению безопасности и стабильности. Кроме того, все чаще вместо обязательной для соблюдения политики выпускаются указания, оставляющие значительную свободу действий в отношении соблюдения требований сторонами, связанными договорными обязательствами, и слабая, обтекаемая и, вероятно, не имеющая средств для ее принудительного исполнения политика. Это прискорбный результат. ВС считает, что сообщество ICANN должно потратить время на разработку политики, которая будет единообразно применяться ко всем регистраторам и регистратурам, а не только к неопределенному подмножеству, действующему по собственной прихоти.

По сути дела, ВС отмечает, что за исключением первой части Рекомендации № 1 (которая обязывает ICANN координировать с техническим сообществом разработку технических стандартов, способствующих разграничению регистрационных данных юридических и физических лиц), итоговый отчет по Фазе 2А EPDP не содержит никакой реальной политики и не налагает никаких обязательств принудительного характера на стороны, связанные договорными обязательствами. Это представляет собой прискорбный провал процесса с участием многих заинтересованных сторон.

⁵¹ https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

Присвоение рабочей группой по EPDP статуса «консенсус» рекомендациям итогового отчета не отражает глубоких разногласий относительно результатов ее деятельности. Очевидно, что значительная часть членов РГ, как и значительная часть сообщества ICANN, считает результаты Фазы 2А неадекватными. Это расхождение во мнениях не следует упускать из виду, даже если РГ настаивает на позиционировании данного отчета как поддержанного на основе консенсуса.

Требование о разграничении юридических и физических лиц

Мы вновь заявляем, что неспособность интернет-пользователей определить, с кем они ведут дела в интернете, и растущая неспособность правоохранительных органов, специалистов по кибербезопасности и юристов находить преступников в интернете по регистрационным данным доменного имени продолжают серьезно подрывать мандат ICANN по обеспечению безопасности и стабильности. Таким образом, интересы этих пользователей не отражены в политике должным образом.

Неспособность группы по EPDP на Фазе 2А достичь консенсуса по вопросу изменения Рекомендации № 17.1 Фазы 1 и ее неспособность «изучить и урегулировать вопрос о проведении различий между физическими и юридическими лицами» в ходе обсуждения, как того требует политика, выработанная на Фазе 1, не означает, что определенная в Рекомендации № 17.1 Фазы 1 политика должна сохраниться или стать политикой ICANN «по умолчанию». На самом деле ситуация противоположная. Поскольку группа на Фазе 2А не смогла достичь консенсуса по этой рекомендации, мы считаем необходимым указать в протоколе, что не было и до сих пор нет согласованного мнения, которое позволило бы регистраторам и регистратурам проводить необязательное разграничение между юридическими и физическими лицами.

Директива NIS2

Развитие Директивы NIS2 свидетельствует о том, что Европейский парламент будет рассматривать и оказывать влияние не только на вопрос о дифференциации юридических и физических лиц, но и на другие вопросы, связанные с WHOIS, включая достоверность, критические элементы данных, своевременную публикацию данных, не относящихся к персональным, и своевременный ответ лицам, подавшим законный запрос на доступ. ICANN должна четко осознать, что основные заинтересованные стороны, в том числе регулирующие органы в Европе и США, внимательно следят за работой Европейского парламента над этими вопросами в рамках NIS2. С достаточной вероятностью можно ожидать заключений и решений судов и органов регулирования в сфере частной жизни, появление которых может ускориться в результате разбирательств, связанных с NIS2. Вполне возможно, что продвижение NIS2 может быстро обогнать разработку политики ICANN, и после ее принятия ICANN потребуется вновь рассмотреть вопрос о влиянии NIS2.

Таким образом, ICANN придется должным образом отреагировать на Директиву NIS2 после ее принятия Европейским Союзом. Это дает ICANN время для обновления своих контрактов и политики, прежде чем NIS2 будет впервые перенесена в законодательство стран-членов ЕС. Неспособность сделать это, скорее всего, приведет к разрозненному и непоследовательному подходу отрасли к выполнению обязательств, предусмотренных Директивой.

Рекомендация № 1

BC не поддерживает эту рекомендацию. Хотя мы поддерживаем обязательство ICANN определить стандартный технический механизм, способствующий дифференциации регистрационных данных юридических и физических лиц, BC сожалеет об отсутствии требования к сторонам, связанным договорными обязательствами, использовать это поле или даже указывать, провели ли они разграничение. Отказ от требования использовать этот технический механизм не приведет к созданию последовательной и надежной RDDS и является упущенной возможностью сократить количество запросов на получение данных, не относящихся к персональным, которые были излишне вымараны, например, контактные данные неаффилированных служб сохранения конфиденциальности/регистрации через доверенных лиц. Такой результат не отвечает потребностям тех, кто занимается расследованием злоупотребления DNS, киберпреступлений, нарушений прав интеллектуальной собственности и других действий, угрожающих благосостоянию потребителей.

Как указано выше, BC твердо убежден, что ICANN должна принять меры по обновлению политики EPDP после принятия Европейским союзом Директивы NIS2.

Рекомендация № 2

BC выступает против Рекомендации № 2 по процедурным основаниям и в том, что касается конкретного содержания этой рекомендации.

С процедурной точки зрения группа по EPDP на Фазе 2А в нарушение Устава ICANN и устава Фазы 2 EPDP необъяснимым образом посвятила значительное время разработке указаний вместо обязательной для соблюдения согласованной политики. Часть членов РГ фактически «тянула время», направив большую часть своих усилий на составление указаний, тем самым отсрочив до последних недель Фазы 2А любое значимое и активное обсуждение выработки обязательной согласованной политики.

Процедура подготовки указаний определена в Приложении 2-А к Уставу ICANN и требует официального запуска Методологического процесса Советом GNSO. Эта процедура не была соблюдена и, как следствие, невозможно подготовить указания на законных основаниях.

В связи с этим определенная в Рекомендации № 2 политика должна быть принята как согласованная политика, а не просто «указания», и должным образом соблюдаться.

Что касается деталей рекомендации, ВС считает, что она также является слабой и неисполнимой, что еще больше ограничивает возможность использования регистрационных данных доменного имени в законных целях. Рекомендация должна требовать от сторон, связанных договорными обязательствами, соблюдения основных положений Рекомендации № 2.

Наконец, мы отмечаем, что на странице 20 итогового отчета допущена ошибка, которая должна быть исправлена следующим образом:

«Это обычно позволяет **публиковать** **раскрывать** данные юридических лиц, поскольку они не входят в сферу действия GDPR; однако при обработке данных юридических лиц стороны, связанные договорными обязательствами, должны принять меры предосторожности, чтобы избежать **публикации** **разглашения** данных, позволяющих идентифицировать физическое лицо, в составе данных, обозначенных как данные юридического лица, поскольку это пример информации, которая входит в сферу действия GDPR».

Эти уточнения необходимы, чтобы обеспечить согласованность с рекомендациями отчета по Фазе 1 EPDP, а именно, что информация о физическом лице **может быть раскрыта по запросу** в законных целях, при наличии правового основания, предусмотренного в GDPR.

Рекомендация № 3

ВС отмечает, что данная рекомендация не определяет ни для одной из сторон никаких обязательств, подлежащих принудительному исполнению, и не поощряет разработку таких обязательств. Рекомендация «рассмотреть» работу по созданию Кодекса поведения в рамках «возможной будущей работы в ICANN» является расплывчатой и неисполнимой; она оставляет без внимания приоритеты сообщества, которые заслуживают должного внимания.

Соответственно, рекомендация должна побудить ICANN начать процесс разработки Кодекса поведения. Если ICANN сделает это, ВС будет решительно возражать против любого процесса, не предполагающего участия всех заинтересованных сторон ICANN. Определение и разработка Кодекса поведения должны осуществляться открытым, транспарентным и инклюзивным образом и этот документ не должен разрабатываться вне процесса ICANN с участием многих заинтересованных сторон (например, путем переговоров за закрытыми дверями между корпорацией ICANN и сторонами, связанными договорными обязательствами).

Рекомендация № 4

Жаль, что группа по EPDP не уделила достаточно времени рассмотрению этой важной темы. ВС по-прежнему считает, что псевдонимный адрес электронной почты с привязкой к владельцу домена должен существовать **в обязательном порядке** для содействия расследованию злоупотребления DNS благодаря возможности контактов с владельцем домена и наличию перекрестных ссылок на домены, принадлежащие одному владельцу.

В очередной раз ВС сожалеет, что в данной рекомендации не определены какие-либо требования к сторонам, связанным договорными обязательствами, что оставляет значительные пробелы между рекомендацией и ее практической реализацией. Рекомендация договорным сторонам оценить юридические рекомендации и риски, выгоды и средства защиты, скорее всего, приведет к чрезмерно осторожной, слабой и в конечном итоге неэффективной политике.

Авторы этого комментария: Алекс Дикон, Марджи Милам, Стив ДельБьянко, Марк Сванкарек, Дрю Беннетт и Мейсон Коул. Он утвержден в соответствии с нашим уставом.

Заявление меньшинства IPC по Фазе 2А EPDP

Законодательство о защите данных, включая GDPR, не распространяется на данные, не относящиеся к персональным. На самом деле, хотя GDPR, по общему признанию, несколько неоднозначен, он может даже не применяться к персональным данным, относящимся к юридическим лицам⁵². Соответственно, в таких базах данных, как WHOIS/RDDS, которые служат множеству целей, представляющих общественный интерес, следует вымарывать только те данные, которые явно являются персональными и требующими особого подхода в соответствии с законодательством о защите данных. Однако на Фазе 2А EPDP «бремя доказательства» или, по крайней мере, «бремя убеждения» было по непонятным причинам неуместно переложено на сторонников здравого смысла, по мнению которых данные, не являющиеся персональными, не должны скрываться. IPC отмечает, что подход к работе на Фазе 2А EPDP изначально был неправильным из-за этого неуместного бремени и стремления подготовить указания вместо обязательной для соблюдения согласованной политики. Дело не только в том, что PDP предназначен для выработки согласованной политики, обязательной в равной степени для всех сторон, связанных договорными обязательствами. IPC также отмечает тревожную тенденцию в разработке политики с участием многих заинтересованных сторон на всех многочисленных этапах EPDP: маловероятен успех, когда некоторые заинтересованные стороны готовы действовать исключительно в своих собственных интересах, мало заботясь о компромиссе в интересах общего блага. Сейчас, как никогда ранее, нам необходимо объединить заинтересованные стороны в интересах безопасности, стабильности и устойчивости DNS и «продвижения глобальных общественных интересов», как указано в Учредительном договоре ICANN. Наконец, мы отмечаем, что обозначение «консенсус», приписываемое рекомендациям Фазы 2А EPDP, неадекватно отражает разногласия в рабочей группе относительно этих результатов, и не отражает того, что Рекомендация № 17.3 по итогам Фазы 1 EPDP «Группа по EPDP изучит и урегулирует вопрос о проведении различий между физическими и юридическими лицами на Фазе 2» остается невыполненной в отсутствие обязательной дифференциации.

Далее следуют конкретные комментарии по Фазе 2А EPDP.

I. Расчет на самоидентификацию владельца домена

Одним из наиболее существенных разочарований с точки зрения здравого смысла в рекомендациях Фазы 2А EPDP является концепция, согласно которой стороны, связанные договорными обязательствами, не должны полагаться на то, что

⁵² «Эти положения не распространяются на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица». GDPR, Преамбула 14

владелец домена сообщает им о характере данных RDS, и либо публиковать, либо вымарывать данные соответствующим образом. Юридическая консультация подтвердила эту оценку, отвечающую здравому смыслу, назвав данные имеющими «низкую степень конфиденциальности», риск «низким», и даже в случае ошибочной публикации на основе неправильного самоназвания владельца домена, «наиболее вероятным представляется предписание исправить проблему (вероятно, сопровождаемое разумным сроком для внесения изменений), а не штраф», обнаружив «отсутствие примеров правоприменения в связи с этим»⁵³.

Действуя на основании такой юридической рекомендации, группа, действительно работающая в общественных интересах, должна была легко согласиться опубликовать данные, которые были идентифицированы субъектом данных как данные, не являющиеся персональными. И все же такого соглашения не появилось.

II. Общий элемент данных

IPC однозначно поддерживает разработку общего элемента — или элементов — данных для отражения того, относятся ли данные RDS к юридическому или физическому лицу-владельца домена и/или содержат ли они персональные данные. Хотя результаты Фазы 2А оказались не самыми впечатляющими, IPC поддерживает и ценит консенсус, достигнутый в рамках модели с участием многих заинтересованных сторон в отношении этого стандартизированного элемента данных.

Тем не менее, IPC и коллеги из других групп интересов и консультативных комитетов твердо убеждены, что такой стандартизированный элемент данных должен быть обязательным, особенно в отсутствие основанной на здравом смысле публикации данных в соответствии с самоидентификацией владельцев доменов. Хотя мы воодушевлены согласием создать этот элемент данных, мы сомневаемся в вероятном положительном влиянии этого компромисса, если такой элемент данных никогда не получит широкого распространения среди сторон, связанных договорными обязательствами. На самом деле, IPC откровенно разочарована и обескуражена тем, что группа на Фазе 2А не смогла договориться о более широком применении этого элемента данных. Возможности варьировались от факультативного сбора данных только для новых доменов до обязательного сбора данных и публикации этого поля для всех доменов, находящихся под управлением. Тем не менее, минимум — необязательный сбор — оказался единственным результатом, по которому удалось достичь консенсуса. Это особенно разочаровывает, учитывая, что само поле не содержит персональных данных, и поэтому нет никакого риска для их публикации. Кроме того, стороны, связанные договорными обязательствами, так и не представили никаких причин для возражений против обязательного сбора или публикации этого элемента данных. Они просто повторили «мы не видим пользы» (предположительно для них как для

⁵³ <https://community.icann.org/display/EOTSFGRD/EPDP+-P2A+Legal+subteam>

регистратур и регистраторов), когда стороны, не связанные договорными обязательствами, представили им обоснование, которое включает: полезность для SSAD, указание на то, следует ли подавать запрос SSAD или единичный запрос регистратуре/регистратору, сведения о том, были ли данные вымараны по существенной причине или из удобства для стороны, связанной договорными обязательствами, и т. д.

III. Будущая работа над Кодексом поведения

Наконец, хотя это потенциально выходило за рамки данной Фазы 2А EPDP, итоговый отчет содержит положение, требующее от ICANN рассмотреть представленные указания по Кодексу поведения при любом будущем взаимодействии с Европейским советом по защите данных. Прежде всего, эта рекомендация является слабой, поскольку не предусматривает создание Кодекса поведения. Кроме того, эта рекомендация сформулирована двусмысленно и охватывает контролеров и обработчиков, а в отдельном предложении упоминается «сообщество». Что еще более тревожно, когда IPC настаивала на включении в итоговый отчет разъяснения, что группы, запрашивающие данные в RDS, должны быть прямо включены в список контролеров и обработчиков (для их собственных целей), некоторые стороны, связанные договорными обязательствами, возражали против этого, ссылаясь на то, что такие отправители запросов представляют «интересы третьих лиц». В среде ICANN с участием многих заинтересованных сторон сообщество, особенно разнообразное сообщество, представленное в GNSO, не должно быть низведено до статуса «наблюдателя» по такому важному вопросу, как правовой статус данных RDS, который является основополагающим для безопасности, стабильности и устойчивости DNS.

IV. Псевдонимный адрес электронной почты с привязкой к владельцу домена

IPC по-прежнему считает, что псевдонимный адрес электронной почты с привязкой к владельцу домена, должен в обязательном порядке публиковаться в WHOIS/RDDS. В юридических рекомендациях, полученных группой на Фазе 2А EPDP, указано, что такая публикация влечет за собой «умеренный» риск, поскольку такие данные в совокупности с другими персональными данными могут быть использованы для идентификации физического лица-владельца домена. Однако преимущества такой публикации для общественных интересов перевешивают права субъекта данных на конфиденциальность, так как возможность использования псевдонимизированных адресов электронной почты с привязкой к владельцу домена имеет решающее значение для содействия обнаружению доменов, принадлежащих одному владельцу, в рамках борьбы с крупномасштабными угрозами безопасности в сетях, фишинговыми схемами и сайтами, нарушающими права на интеллектуальную собственность. Мы отмечаем, что публикация псевдонимизированных адресов электронной почты, привязанных к владельцу домена, по-видимому, соответствует

GDPR, и также отмечаем, что несколько европейских организаций в цепи поставок DNS на самом деле публикуют *фактические* адреса электронной почты владельцев доменов, не нарушая при этом GDPR, как отмечено в полученной группой по EPDP юридической рекомендации⁵⁴. В случае, если Европейский совет по защите данных или отдельный орган защиты данных признает такой подход не соответствующим GDPR, в рамках политики можно вернуть текущее требование о публикации анонимизированного адреса электронной почты или ссылки на веб-форму с раскрытием фактического адреса электронной почты в ответ на обоснованные запросы третьих сторон.

V. Заключение

В заключение следует отметить, что, хотя IPC поддерживает достигнутый консенсус в отношении создания стандартизированного элемента данных для отражения (юридического и физического) статуса владельца домена и/или регистрационных данных, в итоговом отчете по фазе 2А EPDP конечная цель не была достигнута. Рекомендация № 17.3 Фазы 1 EPDP в дополнение к факультативной дифференциации содержала следующее требование: «Группа по EPDP изучит и урегулирует вопрос о проведении различий между физическими и юридическими лицами на Фазе 2». К сожалению, этот вопрос остается нерешенным. Требование к ICANN координировать работу технического сообщества по созданию элемента данных, который стороны, связанные договорными обязательствами, вольны полностью игнорировать, очень трудно назвать «решением» вопроса о дифференциации юридических и физических лиц. А отказ от требования разграничить персональные данные и данные, не являющиеся персональными, не соответствует главной цели EPDP — «сохранить базу данных WHOIS в максимально возможной степени», соблюдая при этом законы о защите конфиденциальной информации.

⁵⁴ «В своей базе данных WHOIS компания EURid публикует адреса электронной почты владельцев доменных имен в TLD .eu (как физических, так и юридических лиц)... Аналогичным образом, хотя организация RIPE-NCC полагается на получение согласия при публикации личной информации о контактных лицах по техническим/ административным вопросам, она публикует информацию персонального характера о владельцах ресурсов на том основании, что «содействие координации между сетевыми операторами является единственной целью, которая оправдывает публикацию персональных данных в базе данных RIPE-NCC, и очевидно, что обработка персональных данных, относящихся к владельцу ресурса, необходима для выполнения функций регистратуры, которая осуществляется в законных интересах сообщества RIPE и бесперебойной работы интернета во всем мире (и потому соответствует статье 6. 1.f GDPR)». Меморандум компании Bird & Bird от 27 апреля 2021 года, первоначальный отчет по Фазе 2А EPDP, стр. 56-57.

Заявление меньшинства GAC относительно окончательного отчета по итогам Фазы 2А Ускоренного процесса формирования политики (EPDP) в области Временной спецификации для регистрационных данных в gTLD

Примечание: Консультативный комитет At-Large (ALAC), Группа интересов коммерческих пользователей (BC) и Группа интересов по вопросам интеллектуальной собственности (IPC) поддерживают мнения, высказанные в этом комментарии.

Введение и общий комментарий

GAC высоко оценивает ответственный подход, продемонстрированный на Фазе 2А группой по EPDP, ее руководством и персоналом поддержки из ICANN, и отдает должное тому, что на разработку этих сложных и важных рекомендаций по политике в области обработки регистрационных данных доменных имен юридических лиц и псевдонимизированных контактных адресов электронной почты, потрачено значительное время. GAC признает полезность многих компонентов итоговых рекомендаций, однако по-прежнему обеспокоен тем, что практически ни одна из этих рекомендаций не создает обязательств, подлежащих исполнению. Поэтому они не соответствуют ожиданиям GAC, что политика потребует публикации регистрационных данных доменного имени, не защищенных согласно Общим положениям о защите данных (GDPR) ЕС, и создания соответствующей структуры для стимулирования публикации псевдонимизированных контактных адресов электронной почты с соответствующими мерами защиты.

Следует понимать, как GAC подчеркивал в своих предыдущих комментариях⁵⁵, что правоохранительным органам и органам защиты прав потребителей, а также другим организациям, занимающимся защитой населения от злонамеренных действий с использованием DNS, необходим быстрый и эффективный доступ к регистрационным данным доменного имени. До мая 2018 года такой доступ можно было получить через систему WHOIS. В ответ на GDPR ICANN внедрила политику, которая позволяет скрывать большую часть этих данных, даже те данные, которые не защищены GDPR. Поскольку GDPR не защищает контактную информацию юридических лиц, многие группы заинтересованных сторон, включая GAC, задались вопросом, почему политика ICANN разрешает вымарывать незащищенную информацию на выходе RDS/WHOIS. Поэтому GAC и другие группы заинтересованных сторон призвали разработать более четкую политику, которая защищала бы персональные данные, но при этом обеспечивала бы публикацию данных, не являющихся персональными, включая регистрационные данные,

⁵⁵ См. Комментарий GAC к итоговому отчету о Фазе 1 EPDP (20 февраля 2019 года), Комментарий GAC к первоначальному отчету о Фазе 2 (24 марта 2020 года) и Комментарий GAC к дополнению к первоначальному отчету о Фазе 2 (5 мая 2020 года). См. также Коммюнике по результатам заседаний GAC в Абу-Даби (1 ноября 2017 года), Коммюнике по результатам заседаний GAC в Сан-Хуане (15 марта 2018 года) и Коммюнике по результатам заседаний GAC в Барселоне (25 октября 2018 года).

относящиеся к юридическим лицам, признавая тем самым, что публикация открытых регистрационных данных доменных имен отвечает общественным интересам.

Круг задач Фазы 2A EPDP учитывал эти проблемы и был сосредоточен на двух темах, а именно:

1. дифференциация регистрационных данных юридических и физических лиц и
2. возможность использования единообразного анонимизированного⁵⁶ адреса электронной почты для индивидуальных контактов.

В рамках первой темы были рассмотрены следующие вопросы:

- i. Необходимо ли изменить соответствующую рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»)⁵⁷;
- ii. Необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие.

В рамках второй темы «возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов», группа по EPDP рассмотрела следующие вопросы:

- i. Имеется ли возможность использования единообразного анонимизированного адреса электронной почты для индивидуальных контактов, и если да, должно ли это стать требованием;
- ii. Если это осуществимо, но не является требованием, какие указания следует дать связанным договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты.

ГАС считает, что в итоговых рекомендациях Фазы 2A есть несколько конструктивных компонентов, в том числе:

1. создание полей данных для обозначения/идентификации владельцев доменов, являющихся юридическими лицами, и персональных данных;
2. конкретные указания о том, какие меры следует принять для защиты персональной информации при разграничении регистрации доменных имен юридическими и физическими лицами;
3. предложение создать Кодекс поведения, который охватывал бы обработку регистрационных данных доменных имен, принадлежащих юридическим лицам;

⁵⁶ Позднее группа по EPDP пришла к выводу, что термин «псевдонимизированный» является более точным. См. «Определения» на стр. 24 [итогового отчета по Фазе 2A EPDP](#).

⁵⁷ См. Рекомендацию № 17 в окончательном отчете по итогам работы группы по EPDP над Фазой 1: <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>.

4. предложение GNSO следить за изменениями в законодательстве, которые могут потребовать пересмотра текущих рекомендаций по политике;
5. полезный контекст и указания для тех, кто хочет публиковать псевдонимизированные адреса электронной почты.

Однако итоговые рекомендации не оправдывают ожиданий, поскольку вместо требований предлагаются в основном факультативные меры даже применительно к информации, которая не защищена GDPR, например, применительно к данным юридических лиц, не относящимся к персональным. Эти факультативные меры могут привести к созданию раздробленной и нечеткой системы для запрашивающих данные лиц и субъектов данных, в которой разными регистраторами применяется различная политика в области защиты или раскрытия данных⁵⁸.

Для справки: значительный процент доменных имен регистрируется юридическими лицами, и GDPR, как правило, не защищает их регистрационные данные доменных имен, не являющиеся персональными. Некоторый анализ показывает, что объем вымаранной регистрационной информации значительно превышает требования GDPR, то есть, «возможно, в пять раз больше необходимого»⁵⁹. Действительно, имеющиеся данные свидетельствуют о том, что физическим лицам, на которых распространяются требования GDPR, могут принадлежать всего около 11,5% доменов, в то время как контактные данные были скрыты для 57,3% всех доменов⁶⁰. Такое, возможно, ненужное скрывание огромного количества регистрационных данных сводит на нет многие преимущества, связанные с транспарентностью владения доменными именами.

Что касается обработки данных юридических лиц, GAC считает, что такая дифференциация должна быть обязательной по многим различным причинам (как отмечено ниже), которые приносят пользу обществу.

Во-первых, публикация регистрационных данных доменных имен юридических лиц, не являющихся персональными данными, увеличит объем информации, доступной организациям, на которые возложена задача защиты общества. Учитывая распространенность интернет-преступлений, публикация регистрационных данных юридических лиц поможет сотрудникам правоохранительных органов, организаций по защите прав потребителей и кибербезопасности быстро и более эффективно расследовать незаконную деятельность с использованием DNS и бороться с киберпреступностью. Кроме того, публикация этих данных позволяет

⁵⁸ GAC выразил свою озабоченность в отношении политики, создающей риск фрагментации, в своих предыдущих комментариях, в том числе в [Коммюнике по результатам заседаний GAC в Барселоне](#) (25 октября 2018 года). См. также [Заявление меньшинства GAC](#) в отношении итогового отчета по Фазе 2 EPDP в области регистрационных данных gTLD (24 августа 2020 года).

⁵⁹ См. основные положения исследования доступности контактных данных WHOIS и классификации владельцев доменов (25 января 2021 года): <https://www.icann.org/en/system/files/correspondence/chapin-to-botterman-25jan21-en.pdf>.

⁶⁰ Тот же источник.

правоохранительным органам и национальным группам реагирования на инциденты информационной безопасности 1) быстро определить юрисдикцию/местонахождение предприятий, ставших жертвами киберпреступлений, и 2) в широких масштабах отправлять юридическим лицам уведомления и защитные сообщения в случае взлома принадлежащих им доменов.

Во-вторых, требование к регистраторам публиковать регистрационные данные доменных имен юридических лиц значительно сократит количество запросов на раскрытие регистрационных данных доменных имен и проблем, связанных с получением ответов на такие запросы⁶¹, поскольку этот массив данных уже будет общедоступным. В-третьих, предоставление общественности данных, не являющихся персональными, в целом повышает доверие к DNS, обеспечивая прозрачность владения доменными именами, в том числе доменами, которые способствуют конфиденциальным онлайн-коммуникациям и сделкам.

Наконец, в полученных юридических рекомендациях подчеркиваются низкие риски, связанные с регистрационными данными юридических лиц. Персональная информация, которая включена в регистрационные данные юридических лиц, скорее всего, будет иметь «низкую степень конфиденциальности», поскольку относится к рабочим данным сотрудника, а не к его личной жизни⁶². Более того, при соблюдении надлежащих мер предосторожности юридические риски, связанные с публикацией таких данных даже в случае непреднамеренных ошибок, представляются незначительными⁶³.

В целом, мы считаем, что процесс разграничения данных юридических и физических лиц сторонами, связанными договорными обязательствами, должен носить обязательный характер. В итоговом отчете недостаточно отражены различные интересы, стоящие на кону при обсуждении дифференциации и последующей публикации незащищенной информации. GAC считает, что общественные интересы перевешивают коммерческие соображения, особенно потому, что общедоступная информация будет способствовать стабильности, безопасности и отказоустойчивости DNS.

В приведенных ниже комментариях указаны конкретные опасения в отношении итоговых рекомендаций.

⁶¹ См. раздел 5.3.1 [проекта отчета](#) группы по анализу RDS (31 августа 2018 года) и результаты [совместного опроса](#), проведенного Антифишинговой рабочей группой и Рабочей группой по борьбе со злоупотреблением рассылкой сообщений (18 октября 2018 года).

⁶² См. [меморандум компании Bird & Bird](#) от 6 апреля 2021 года.

⁶³ Тот же источник.

Рекомендация № 1. Поля для содействия разграничению регистрационных данных юридических и физических лиц

GAC настаивал на создании и использовании полей данных для маркировки владельцев доменов-юридических лиц и наличия или отсутствия персональной информации в их наборах данных. Такие механизмы маркировки стали бы необходимым первым шагом для дифференциации. Рекомендация № 1 содержит ряд обязательств по созданию полей, способствующих разграничению регистрационных данных юридических и физических лиц и определению того, содержат ли эти регистрационные данные персональные данные или данные, не относящиеся к персональным. Помимо создания этих полей вводятся и другие обязательства:

- для ICANN — координировать разработку техническим сообществом, например рабочей группой по RDAP, всех необходимых для такого поля (полей) стандартов;
- для SSAD — в соответствии с рекомендациями Фазы 2 EPDP поддерживать эти поля для содействия интеграции между SSAD и системами сторон, связанных договорными обязательствами; и
- для полей — поддерживать конкретные значения, связанные со статусом юридических лиц и наличием или отсутствием персональных данных.

GAC особенно высоко оценивает точность определения в данной рекомендации того, какие значения должны находиться в этих полях. Однако GAC считает, что Рекомендация № 1 была бы более эффективной в создании необходимой инфраструктуры для дифференциации, если бы она:

1. требовала от сторон, связанных договорными обязательствами, не только создавать, но и использовать эти поля;
2. устанавливала конкретные сроки приведения этих полей в рабочее состояние; и
3. обеспечивала функционирование этих полей в рамках существующих и проектируемых систем сбора и раскрытия данных.

Во избежание разночтений следует уточнить, что GAC считает требование к сторонам, связанным договорными обязательствами, заполнять эти поля для всех будущих регистраций, независимо от того, выбирают ли стороны, связанные договорными обязательствами, дифференцированный подход к данным физических и юридических лиц, эффективным и отвечающим общественным интересам, поскольку это создаст основу для маркировки и идентификации данных, которые могут стать предметом будущих ускоренных запросов к SSAD или будущих юридических обязательств⁶⁴.

⁶⁴ В этой связи GAC приветствует содержащийся в итоговом отчете призыв к GNSO оценить необходимость дальнейшей работы над политикой в свете изменений законодательства. Например, группа по EPDP отметила текущие обсуждения и ожидаемое принятие уточненной редакции Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем («NIS2»). См. «Предложение Совету GNSO» на стр. 15 [итогового отчета по Фазе 2А EPDP](#).

ГАС также отмечает, что добровольное использование такого поля не соответствует результатам предыдущих фаз EPDP, на которых такие меры, как вымарывание данных, применялись ко всей системе, вместо того, чтобы полагаться на индивидуальные решения сторон, связанных договорными обязательствами.

Рекомендация № 2. Указания для сторон, связанных договорными обязательствами, решившим проводить дифференциацию

Группа по EPDP разработала указания по дифференциации на основе применимых принципов GDPR и обширных юридических консультаций. Примечательно, что в юридических рекомендациях определены очень конкретные меры предосторожности для снижения риска неправомерного раскрытия информации и отмечено, что в любом случае данные, о которых идет речь, не являются столь же конфиденциальными, как другие категории персональной информации, поскольку относятся к работе, а не к личной жизни. Наконец, в юридических рекомендациях отмечено, что в случае соблюдения мер предосторожности даже непреднамеренное раскрытие личной информации вряд ли приведет к правоприменительным действиям. Поскольку в указаниях приняты рекомендованные меры предосторожности, возникающие риски ответственности низки, а польза для общества, как уже говорилось, высока.

По указанным выше причинам ГАС считает, что эта рекомендация должна была требовать от сторон, связанных договорными обязательствами, проводить различие между юридическими и физическими лицами и, соответственно, также требовать от сторон, связанных договорными обязательствами, использовать надлежащие указания, изложенные в Рекомендации № 2, и публиковать в общедоступных источниках все данные юридических лиц, не являющиеся персональными. ГАС также считает, что меры предосторожности, отраженные в Рекомендации № 2, уместнее называть «передовой практикой».

Рекомендация № 3. Кодексы поведения и примеры сценариев

ГАС приветствует рекомендацию группы по EPDP о том, что изложенные в Рекомендации № 2 указания группы следует учесть при возможной будущей разработке в ICANN соответствующими контролерами и обработчиками Кодекса поведения GDPR. ГАС отмечает, что заинтересованным сторонам, которых затрагивает такой кодекс, в том числе потенциальным отправителям запросов на получение (и, следовательно, потенциальным обработчикам) регистрационных данных доменных имен, должна быть предоставлена возможность участия в разработке кодекса.

ГАС также высоко оценивает указания, предложенные для конкретных сценариев. ГАС считает, что логика и ясность этих трех сценариев была бы выше, если бы они

требовали публикации или неразглашения информации. В каждом сценарии описаны конкретные условия, которые логически предписывают либо публикацию, либо неразглашение регистрационных данных доменных имен, и поэтому использование слова «следует» вместо «обязан» в этих сценариях является неуместным.

Рекомендация № 4. Псевдонимизированные адреса электронной почты

Что касается индивидуальных контактов и псевдонимизированных адресов электронной почты, GAC приветствует шаги по предоставлению указаний о публикации адреса электронной почты с использованием метода защиты данных путем применения различных способов анонимизации и отмечает пониженный уровень риска, который обеспечивает такая публикация, что подчеркивается в полученных группой по EPDP юридических рекомендациях⁶⁵. Хотя GAC признает существование определенных рисков в связи с публикацией даже псевдонимизированной информации, статья 28 GDPR подчеркивает возможность использования псевдонимизации в качестве метода снижения этих рисков для субъектов данных и содействия контролерам и обработчикам в выполнении их обязательств по защите данных. Более того, псевдонимизированные адреса электронной почты широко используются для оказания услуг сохранения конфиденциальности и регистрации через доверенных лиц. При этом многие субъекты данных практически не ощущают их влияния. GAC также отмечает преимущества, которые обеспечит такая публикация псевдонимизированных адресов электронной почты, особенно в отношении содействия быстрой и эффективной связи с владельцами доменных имен. Поступали сообщения о том, что некоторые веб-формы не являются эффективными механизмами общения с владельцами доменов.

⁶⁵ См. меморандум компании Bird & Bird от 9 апреля 2021 года [Варианты маскирования адреса контактного лица](#) и меморандум компании Bird & Bird от 4 февраля 2020 года [Вопросы по Системе обеспечения стандартизованного доступа к закрытым регистрационным данным gTLD и их раскрытия \(«SSAD»\), сохранению конфиденциальности/регистрации через доверенных лиц и псевдонимизированным адресам электронной почты.](#)

**Заявление меньшинства NCSG относительно окончательного
отчета по итогам Фазы 2А EPDP**

NCSG рада, что последние задачи фаз 1 и 2 EPDP выполнены. Мы также рады, что ICANN наконец-то соблюдает закон о защите данных, чего мы добивались с самых первых дней обсуждения политики WHOIS. Однако этот EPDP был неоправданно долгим и болезненным и отражает не столько осознание ответственности ICANN за соблюдение закона о защите данных, сколько трудности принятия многими заинтересованными сторонами концепции уважения прав владельцев доменов. Мы также считаем, что распространение заявлений меньшинства, в которых еще раз изложены позиции, которые неоднократно высказывались в течение как минимум последних девяти месяцев, если не последних трех лет, является излишним. Однако NCSG не готова идти на принцип и отказываться от возможности напомнить свои собственные доводы.

Мы неоднократно поднимали вопрос о правах владельцев доменов. Обычно мы были одиноки, когда речь заходила о правах владельцев доменов; к нам следовало присоединиться как минимум ALAC, SSAC и GAC, у которых есть четкие функции защиты прав владельцев доменов. К счастью, стороны, связанные договорными обязательствами, также поддерживают своих клиентов и регулярно указывают на свои обязательства перед ними. ICANN также должна подчеркивать права клиентов как беспристрастный посредник при выработке сообществом многих заинтересованных сторон принципов управления gTLD.

Отсутствие ясности насчет роли корпорации ICANN как одного из контролеров, совместно отвечающих за обработку данных, также вносит неразбериху и усложняет понимание политики. Мы часто заявляли о необходимости в самом начале этой работы уточнить конкретный характер функций ICANN и сторон, связанных договорными обязательствами, несомненно, с привлечением внешнего юридического консультанта. Характер соглашений о совместном контроле очень важен; можно было бы сэкономить много времени и избежать путаницы, если бы мы были лучше осведомлены об этих возможных договорных отношениях.

Ряд сторон подняли вопрос о европейских законопроектах, которые могут повлиять на применение GDPR, и это замедлило процедуру. Мы считаем, что не следует пытаться изменить результаты работы, проделанной на первых двух фазах EPDP, исходя из предположений о возможном регулировании. Кроме того, желание ограничить внедрение GDPR за несколько лет до того, как такие нормативные акты будут приняты и закреплены в национальных законах, указывает на неспособность принимать во внимание закон о защите данных и права владельцев доменов на частную жизнь.

Что касается конкретных вопросов, рассматриваемых в данном отчете, то мы подчеркивали на протяжении всего EPDP, а также во время предыдущего PDP в

области услуг сохранения конфиденциальности и регистрации через доверенных лиц, что проведение различия между юридическими и физическими лицами не приносит пользы при принятии решения о необходимости защиты данных в RDS. Как мы уже неоднократно повторяли, такая постановка вопроса неверна, поскольку у многих работников, нанятых юридическим лицом или компанией, есть права на неприкосновенность частной жизни в отношении раскрытия их личных и контактных данных. У юридического лица нет прав на неприкосновенность частной жизни, но у людей они есть.

Даже если дополнить вопрос о «разделении на юридических и физических лиц» уточняющим вопросом, требующим, чтобы владелец домена подтвердил отсутствие личных данных в предоставленной им информации, это никоим образом не устранил риск раскрытия личной информации. На оба вопроса трудно ответить многим организациям, особенно тем, которых представляет NCSG, то есть некоммерческим и волонтерским организациям, клубам и группам по интересам, религиозным группам, правозащитным организациям и так далее.

Это также относится к индивидуальным подрядчикам, некоторым видам специалистов и фрилансерам, которые рассматриваются как подрядчики, но на самом деле трудятся в рамках отношений «работодатель/работник». Если крупные корпорациям с юридическими отделами, даже те, которые ведут широкую и глобально распределенную деятельность, могут без особого труда ответить на этот вопрос, то для небольших организаций с меньшим бюджетом и некорпоративным способом взаимодействия со своими волонтерами и членами это не так просто.

Поэтому наша позиция такова: поскольку для многих организаций такое разграничение не является четким, нецелесообразно и нежелательно вводить его в обязательном порядке, и хотя стороны, связанные договорными обязательствами, разработали прекрасные указания для своих членов, чтобы помочь им решить задачу такого разграничения, эти указания не должны быть частью политики. В составе политики это станет указаниями по правовым вопросам, которые ICANN не должна давать. Стороны, связанные договорными обязательствами, вполне способны опубликовать эти указания самостоятельно, а ICANN вполне может расценивать их как передовой опыт частного сектора, а не как указания, предусмотренные их политикой, соблюдение которых контролирует ICANN. Стороны, связанные договорными обязательствами, должны лучше остальных понимать свои правовые риски, и поскольку они являются контролерами и несут ответственность за любые штрафные санкции, которые могут налагаться в результате правоприменительных действий, то им следует предоставить свободу принятия решений о том, как управлять раскрытием информации о клиентах.

Мы отмечаем, что те стороны, которые больше всего настаивали на проведении различия между юридическими и физическими лицами, также настаивали на создании поля или полей для ввода данных. Учитывая сохранение рекомендации

о том, что это добровольное для применения поле, и только от самих связанных договорными обязательствами сторон, бизнес-модели которых сильно разнятся, зависит, как они будут использовать это поле (поля), мы не считаем полезными рекомендации о точности данных в этом поле. ICANN принимает на себя обязательство проинструктировать IETF, например, о том, как стандартизировать поле, каким образом сохранить добровольный характер этого разграничения, а также сбора и раскрытия соответствующих данных, необходимых для проведения этого разграничения? Этот вопрос следует оставить для передовых практик частного сектора.

Мы также выступаем за права фрилансеров, индивидуальных подрядчиков и независимых творческих работников, продавцов и профильных специалистов, несмотря на то, что по уставу мы представляем интересы некоммерческих заинтересованных сторон. Никто другой не представляет интересы этих людей, число которых стремительно растет по мере того, как модели занятости меняются вместе с глобальной интернет-экономикой. Этот разрыв красноречиво говорит об акценте на крупный бизнес и отсутствии внимания к проблемам конкуренции, которые усугубляются политикой DNS. Мы надеемся, что стороны, связанные договорными обязательствами, будут учитывать права этих лиц и внимательно следить за тем, чтобы при реализации данной политики с ними обращались справедливо и с должным уважением к нормам конфиденциальности.

Группа заинтересованных сторон-регистраторов

Представители группы заинтересованных сторон-регистраторов (RrSG) в рабочей группе (РГ) по Фазе 2А EPDP благодарят персонал ICANN и всех остальных участников РГ EPDP за упорную работу на этой фазе EPDP. Следующее заявление призвано дополнить наше голосование в рамках определения консенсуса и комментарии в ходе работы над Фазой 2А EPDP.

Комментарии общего характера

В течение всего обсуждения на Фазе 2А EPDP группа RrSG подчеркивала, что каждый отдельно взятый регистратор должен иметь возможность определить уровень риска, который он принимает на себя в рамках базового уровня, позволяющего соблюдать соответствующие юридические обязательства. Аналогичным образом, каждый отдельно взятый регистратор должен иметь возможность определить, что он считает коммерчески и технически возможным для своего уникального бизнеса.

Хотя рекомендации, предложенные РГ по EPDP на Фазе 2А позволяют осуществить такое самоопределение, предоставляя варианты и указания тем регистраторам и регистратурам, которые решили проводить разграничение на основе наличия персональных данных в регистрационной записи или решили публиковать контактный адрес электронной почты с привязкой к владельцу домена или регистрации, досадно, что этот результат был достигнут только после серьезной

борьбы. В ходе работы над этой фазой РГ неоднократно возвращалась к одним и тем же вопросам, не добавляя ничего существенно нового к обсуждению, и обсуждала темы, выходящие за рамки круга задач. Пожалуй, наиболее важно, что РГ во многих случаях не интересовали правовые и финансовые риски, которые некоторые предлагаемые обязательства создадут для сторон, связанных договорными обязательствами, в различных юрисдикциях или с различными бизнес-моделями, или риски для самих владельцев доменов.

Наконец, мы отмечаем, что любые потенциальные преимущества императивных обязательств в этих областях политики, которые свели бы на нет важнейшую возможность регистраторов выбирать собственные юридические, коммерческие и технические риски, не были продемонстрированы достаточно четко или убедительно, чтобы показать абсолютную необходимость таких обязательств по сравнению с менее проблематичными вариантами, предложенными группой регистраторов. Предложенные обязательства по соблюдению политики не были основаны на строгой необходимости или широко признанных улучшениях экосистемы доменов, которые оправдывали бы введение подобных требований. Поэтому группа RrSG уверена, что результат работы на Фазе 2А, включая указания и необязательные требования по дифференциации и использованию адреса электронной почты, привязанного к владельцу домена или регистрации, является надлежащим результатом.

Дифференциация юридических и физических лиц

Группа RrSG поддерживает сохранение Рекомендации № 17 (1) Фазы 1 и считает это решением проблемы, упомянутой в Рекомендации № 17 (3) Фазы 1. Хотя различные группы, представленные в РГ по EPDP на Фазе 2А, не пришли к согласию по этому вопросу, все соответствующие материалы были изучены и подробно рассмотрены в ходе дискуссий, и дальнейшее обсуждение не планируется и не ожидается; то есть вопрос был решен. Более того, это *правильное* решение. Каждый регистратор должен самостоятельно проводить анализ соотношения между риском и выгодой и учитывать свою уникальную правовую среду, чтобы определить, будет ли он проводить дифференциацию и каким образом, и эта рекомендация дает ему такую возможность.

Группа регистраторов подчеркивает, что метод дифференциации у разных регистраторов будет различаться. Как использование «меток» или «полей» для указания типа лица или наличия персональных данных, так и содержание самих указаний рассматривается в рамках данной фазы как факультативное, а не обязательное для всех регистраторов. Данные указания носят высокоуровневый характер и являются результатом значительного компромисса; они полезны, но не применимы во всех ситуациях или ко всем регистраторам мира. Поэтому они *должны* оставаться необязательными. Любые обязательные указания или Кодекс поведения могут быть созданы только самими соответствующими сторонами, связанными договорными обязательствами, с учетом вклада сообщества.

Возможность индивидуальных контактов

Группа RrSG согласна, что публикация в общедоступной RDDS адреса электронной почты с привязкой к регистрации или владельцу домена является обработкой данных, и выражает признательность компании Bird & Bird за полезный и подробный вклад в рассмотрение этого вопроса. Хотя некоторые варианты реализации такой публикации могут быть менее рискованными, чем другие, мы еще раз отмечаем, что у каждого регистратора должна быть возможность самостоятельно определить степень, в которой он берет на себя юридические риски, и членам РГ по EPDP на Фазе 2А не следует принимать за них это решение. Соответственно, мы рекомендуем всем читателям настоящего итогового отчета ознакомиться с юридическими рекомендациями по данной теме (включенным в качестве Приложения F к итоговому отчету), и ожидаем, что дальнейшие указания и поддержка будут предоставляться членам группы заинтересованных сторон-регистраторов по мере необходимости.

Для более подробного ознакомления с мнением группы RrSG по этим темам предлагаем также обратиться к нашей заметке на сайте Circle ID:

[Конфиденциальность, дифференциация юридических и физических лиц и бесконечный EPDP ICANN](#). Спасибо.

Группа заинтересованных сторон-регистратур

Заявление меньшинства относительно окончательного отчета по итогам работы над Фазой 2А ускоренного процесса формирования политики по Временной спецификации для регистрационных данных в gTLD

После более чем трехлетних усилий RySG с удовлетворением отмечает завершение ускоренного процесса формирования политики по Временной спецификации для регистрационных данных в gTLD («EPDP»). Это были практически беспрецедентные усилия, вызванные вступлением в силу регламента GDPR, который потребовал от сообщества ICANN объединить усилия для устранения давних несовместимостей с обязательствами по защите данных. RySG невероятно благодарна за упорную работу и целеустремленность нашим председателям и их заместителям, неутомимой группе поддержки из числа персонала ICANN и членам группы по EPDP, которые добросовестно стремились достичь взаимопонимания по этим, безусловно, сложным темам.

RySG уверена, что, как и на предыдущих этапах этой работы, мы нашли надлежащий баланс между защитой прав субъектов данных на конфиденциальность, выполнением наших юридических обязательств и отсутствием ненужных препятствий или операционных проблем для наших клиентов или наших предприятий.

I. Проблема дифференциации юридических и физических лиц решена

На Фазе 2А была решена проблема дифференциации юридических и физических лиц. Чтобы решить проблему, PDP не обязательно должен привести к согласованным рекомендациям. То, что рабочая группа не пришла к согласию по поводу изменения предыдущей рекомендации (Фаза 1, Рекомендация № 17) о проведении различия между юридическими и физическими лицами, является ценным и приемлемым результатом. После трех фаз обсуждения в рамках EPDP, исследования, проведенного корпорацией ICANN, и правовых рекомендаций внешних юристов по вопросу дифференциации юридических и физических лиц, уже давно пора признать этот вопрос закрытым.

Действительно, группа по EPDP постаралась выполнить поручение Совета GNSO «ответить на вопрос . . . необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»)»⁶⁶. Ответ на этот

⁶⁶ Поручения Совета GNSO по работе над вопросом о дифференциации юридических и физических лиц на Фазе 2А: «Ожидается, что группа по EPDP рассмотрит предпринятое корпорацией ICANN исследование (выполненное по просьбе группы по EPDP и одобренное Советом GNSO во время Фазы 1) наряду с юридическими рекомендациями компании Bird & Bird, а также предложениями по существу данного вопроса, поступившими в ходе общественного обсуждения, и ответит на следующие вопросы

конкретный вопрос требует рассмотрения в полном объеме Рекомендации № 17 Фазы 1, состоящей из трех частей⁶⁷. Доводы о том, что группа по EPDP не выполнила пункт 17.3 («Группа по EPDP изучит и урегулирует вопрос о проведении различий между физическими и юридическими лицами на Фазе 2»), представляют собой намеренно узкий взгляд на содержание этой рекомендации, игнорирующий четкие поручения Совета GNSO. RySG обеспокоена тем, что некоторые предполагают, будто этот вопрос не решен. Указанный вопрос обсуждался на трех отдельных фазах EPDP, и каждый раз результатом было то, что стороны, связанные договорными обязательствами, могут проводить различия, но не обязаны это делать. Это наглядно демонстрирует, что данный вопрос решался надлежащим образом и последовательно. Мнение о том, что какая-то часть этой работы не завершена, может нанести ущерб сообществу ICANN и рассматриваться как подрыв эффективности модели с участием многих заинтересованных сторон. Это было бы также несправедливо по отношению к членам рабочей группы и огромному количеству времени, которое они потратили на обсуждение и решение этого вопроса.

II. Необязательная дифференциация остается хорошим результатом

RySG твердо убеждена, что сохранение разрешительных, но не обязательных рекомендаций Фазы 1⁶⁸ в отношении регистрационных данных юридических и физических лиц является объективно хорошим результатом нашей деятельности по разработке политики. Такой результат не подразумевает простое сохранение статус-кво. Мы считаем чрезвычайно важным баланс, достигнутый в формулировке Рекомендации № 17 Фазы 1 (после серьезного рассмотрения), особенно учитывая

- I. Необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»);
- II. Необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие».

⁶⁷ [Итоговый отчет по Фазе I EPDP](#) содержит следующую рекомендацию по вопросу дифференциации юридических и физических лиц: **Рекомендация № 17.1:** «Группа по EPDP рекомендует разрешить регистраторам и операторам регистратур проводить различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, но не рекомендует вменять им это в обязанность».

Рекомендация № 17.2: «Группа по EPDP рекомендует корпорации ICANN на основе мандата, разработанного по согласованию с сообществом, как можно скорее выполнить исследование:

- осуществимости дифференцированного подхода к юридическим и физическим лицам и расходов, включая расходы на реализацию и расходы в связи с возможной юридической ответственностью;
- примеров отраслей или других организаций, где используется дифференцированный подход к юридическим и физическим лицам;
- рисков для конфиденциальности владельцев зарегистрированных имен, возникающих в связи с дифференцированным подходом к юридическим и физическим лицам; и
- других потенциальных рисков (если таковые имеются) для регистраторов и регистратур, возникающих в связи с отсутствием дифференцированного подхода».

Рекомендация № 17.3: «Группа по EPDP изучит и урегулирует вопрос о проведении различий между физическими и юридическими лицами на Фазе 2».

⁶⁸ Рекомендация № 17.1: «Группа по EPDP рекомендует разрешить регистраторам и операторам регистратур проводить различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, но не рекомендует вменять им это в обязанность».

неопределенность регулирования, на которую многие члены группы по EPDP неоднократно ссылались как на обоснование необходимости изменения этой рекомендации Фазы 1. Напротив, именно из-за этой неопределенности Рекомендация № 17 является подходящим, гибким и элегантным решением вопроса о дифференциации юридических и физических лиц.

а. Сторонам, связанным договорными обязательствами, необходимо дать возможность самостоятельно контролировать свои правовые риски

Как объясняла RySG на всем протяжении Фазы 2А, гибкость, присущая разрешению на дифференциацию, но при отсутствии требования о дифференциации, важна для того, чтобы позволить сторонам, связанным договорными обязательствами, контролировать свои собственные правовые риски и снижать риски для своих клиентов. Регистратуры и регистраторы неоднократно заявляли об этом как о фундаментальной предпосылке на протяжении всего EPDP.

В юридических меморандумах четко указано: «если у соответствующих сторон нет причин сомневаться в надежности самоидентификации владельца домена, то они, вероятно, могли бы полагаться только на самоидентификацию без независимого подтверждения. Однако мы понимаем, что стороны обеспокоены тем, что некоторые владельцы доменов не поймут вопрос и будут ошибочно идентифицировать себя. Поэтому возникнет риск ответственности, если соответствующие стороны не предпримут дополнительных шагов для обеспечения точности обозначения владельца домена»⁶⁹. Аналогично, «если существует обоснованный риск ошибок субъектов данных при самоидентификации, то неспособность довести до сведения субъектов данных последствия самоидентификации может привести к ответственности за несоблюдение принципа законности, справедливости и транспарентности»⁷⁰.

RySG высоко оценивает то, что компания Bird & Bird предоставила указания по снижению этих рисков. Однако ответственность за принятие решения о том, каким образом внедрять эти процедуры, не говоря уже об определении уровня приемлемого и неприемлемого риска, должна лежать исключительно на сторонах, связанных договорными обязательствами, которые несут этот риск. В рамках любой другой коммерческой договоренности этот тезис не вызвал бы никаких споров. Как мы говорили с самого начала данного PDP, в тех случаях, когда стороны, связанные договорными обязательствами, несут ответственность за обработку данных, решения относительно этих данных должны приниматься регистратурами и

⁶⁹ «Консультация по вопросам ответственности в связи с самоидентификацией владельца домена как физического или юридического лица в соответствии с Общими положениями о защите данных (Регламент (ЕС) 2016/679) («GDPR»)», Рут Бордман (Ruth Boardman) и Гейб Малдофф (Gabe Maldoфф), от 25 января 2019 года: <https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx>

⁷⁰ Тот же источник

регистраторами, а не третьими лицами, которые сами не несут никакого риска и не имеют общих интересов в отношении защиты данных наших клиентов.

b. Желательная гибкость

Сохранение гибкой, а не предписывающей политики в отношении дифференциации юридических и физических лиц дает регистраторам и регистратурам свободу маневра и возможность быстро реагировать на будущие нормативные изменения, которые могут повлиять на публикацию данных о юридическом лице, без необходимости дополнительной работы по определению политики. RySG признает, что [Уточненная редакция Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем \(«NIS 2»\)](#) после принятия может повлиять на обработку данных юридических лиц регистраторами и регистратурами. Неопределенность в отношении того, как и когда государства-члены ЕС будут внедрять NIS 2, как раз и является причиной того, что регистратурам и регистраторам необходима гибкость для самостоятельного определения способов соблюдения требований в изменчивой нормативно-правовой среде. Меняющаяся и развивающаяся картина в области сохранения конфиденциальности подкрепляет рекомендацию Фазы 1, которая подтверждает возможность сторон, связанных договорными обязательствами, проводить различие между юридическими и физическими лицами.

c. Недостаточное обоснование того, что дополнительные требования необходимы или хотя бы полезны

Несмотря на то, что RySG решительно поддерживает Рекомендацию № 17 Фазы 1 по существу, мы также отмечаем, что не было представлено убедительное обоснование того, почему обязательная дифференциация была бы необходима или хотя бы желательна. Без дополнительной информации мы не можем точно понять, какую проблему пытается решить обязательное разграничение между регистрациями юридических и физических лиц.

III. RySG доверяет процессу GNSO в том, что касается оценки необходимости дальнейшей работы над политикой

RySG поддерживает предложение предупредить Совет GNSO о необходимости постоянного мониторинга NIS 2. Однако мы не считаем, что проект NIS 2 в его текущем виде требует новой работы над политикой, и сомневаемся в том, что такой результат предопределен. RySG поддерживает и признает роль Совета GNSO в определении того, когда необходима работа над политикой. Практика и процедуры GNSO ясно дают понять, что политика ICANN не должна дублировать обязательства, которые стороны, связанные договорными обязательствами, несут по закону. ICANN инициировала этот EPDP для решения проблемы вступления в силу GDPR, работа над политикой в этом случае была необходима из-за прямых

конфликтов между требованиями в наших соглашениях с ICANN и требованиями GDPR. То же самое нельзя сказать о законопроекте NIS 2. Тем временем в Калифорнии, Вирджинии, Японии, Индии и Китае (и это лишь несколько примеров) были приняты или вступили в силу законы о защите данных, которые должны соблюдаться некоторыми или всеми сторонами, связанными договорными обязательствами. Никто не предложил (с полным на то основанием), чтобы ICANN разработала политику для обеспечения соблюдения этих обязательств, потому что нет прямых конфликтов с нашими соглашениями. В конечном итоге решение о необходимости и сроках начала новой работы над политикой должно быть оставлено за Советом GNSO в соответствии с действующими процедурами.

IV. Рекомендация №1 выходит за установленные рамки и поднимает важные вопросы, касающиеся ее выполнения

Напомним, что относительно дифференциации юридических и физических лиц Совет GNSO поручил группе по EPDP на Фазе 2А ответить на два простых и конкретных вопроса: (1) необходимо ли изменить рекомендацию по итогам Фазы 1 EPDP («Разрешить регистраторам и операторам регистратур проводить различия между регистрациями в зависимости от того, выполняются ли они физическими или юридическими лицами, но не вменять это в обязанность»); и (2) необходимо ли дать указания регистраторам и/или регистратурам, проводящим различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, и если да, то какие⁷¹.

Соблюдение согласованных рамок PDP имеет принципиально важное значение для выработки эффективной политики. К сожалению, работа над вопросами Фазы 2А пострадала от постоянных попыток расширить круг наших задач, которые в конечном итоге привели к появлению рекомендации о создании нового элемента данных, выходящей, как мы неоднократно отмечали, за рамки указаний Совета GNSO. Обязательное создание нового элемента данных никак не связано с формулировкой Рекомендации №17 Фазы 1 и поэтому не может считаться ответом на первую часть задачи, поставленной перед нами GNSO. Вместо того чтобы обратиться за разъяснением круга задач в самом начале рассмотрения этого вопроса, председатель группы по EPDP решил, что создание такого элемента данных относится к указаниям, входящим в объем работ EPDP. Более того, «если Совет GNSO решит, что наша работа выходит за рамки, он сообщит об этом»⁷².

⁷¹ Устав Фазы 2А GNSO доступен здесь: <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf>

⁷² «Что касается вашего вопроса о круге задач, то руководство и персонал обсудили это. Я считаю, что то, что мы здесь обсуждаем в отношении указаний, находится в рамках устава EPDP, полученных нами указаний и вопросов, которые были перед нами поставлены. И я думаю, если Совет GNSO решит, что наша работа выходит за рамки, он сообщит об этом. В состав группы входит его представитель, Филипп, который также является председателем GNSO и будет решать любые вопросы, связанные со кругом задач». Председатель EPDP, заседание Фазы 2А, 5 августа 2021 года.

В связи с этим RySG убедительно просит Совет GNSO перед рассмотрением вопроса об утверждении рекомендации сначала рассмотреть Рекомендацию №1 на предмет того, действительно ли данное предложение входит в круг задач Фазы 2А. Как мы объяснили, по нашему мнению, не входит. Даже если GNSO решит, что Рекомендация №1 входит в круг задач, у группы RySG останутся значительные сомнения в ее целесообразности и опасения насчет ее практической реализации.

а. Рекомендация №1 не связана с полученными от Совета поручениями

Мы считаем, что предлагаемое обязательное создание нового элемента данных, которое требует взаимодействия с IETF и, вероятно, дополнительного взаимодействия в других областях, не является «указанием», упомянутым в поручениях GNSO. Существование (или отсутствие) стандартизированного элемента данных не помогает сторонам в процессе дифференциации, а лишь фиксирует результат этого процесса. Сосредоточение внимания на результате, а не на процессе, не является указанием, по крайней мере, существенным практическим указанием, и поэтому не соответствует поручениям Совета касательно EPDP.

Аналогичным образом, рассматривая возможность создания стандартного элемента данных, мы не согласны, что рекомендация о новом элементе данных относится к указаниям просто потому, что элемент данных упоминается в этих указаниях. Нельзя подобным образом включать дополнительные пункты в круг задач PDP. EPDP не должен выходить за рамки соответствующих поручений, и наши рекомендации должны быть столь же целенаправленными.

б. Создание нового элемента данных поднимает существенные вопросы реализации

Даже если GNSO решит, что Рекомендация №1 входит в круг задач Фазы 2А, группа RySG считает, что есть существенные вопросы реализации, которые GNSO и ICANN должны тщательно рассмотреть до принятия этой рекомендации.

ICANN не сможет создать предлагаемый элемент данных самостоятельно. Интернет-стандарты EPP и RDAP (технические спецификации), которые являются основой для большинства каналов связи, используемых для регистрационных данных, контролируются IETF. IETF имеет независимый от ICANN процесс в рамках технического сообщества, состоящего не только из сторон, связанных с ICANN, что потенциально создает проблемы с реализацией.

Учитывая значительную озабоченность, возникшую в связи с принятием этого элемента данных, мы отмечаем, что не было представлено убедительного обоснования того, почему этот элемент данных является необходимым или полезным, особенно в рамках общедоступной RDDS. Выдвинутые аргументы, включая (i) отслеживание того, в какой степени стороны, связанные договорными обязательствами, осуществляют дифференциацию; (ii) предоставление общественности возможности проверить точность обозначения статуса юридического и физического лица; (iii) оценка соблюдения применимых законов;

(iv) упоминаемое мимоходом «единообразие» и (v) вопрос «какой вред может быть от внедрения этого элемента данных?», не имеют практической пользы, и подобные результаты, скорее всего, достижимы с помощью уже существующих механизмов. Ни один из представленных аргументов не имеет практического смысла, не говоря уже о необходимости или убедительности, чтобы оправдать столь значительные и выходящие за рамки существующей политики изменения.

Как указано выше, наличие (или отсутствие) стандартизированного элемента данных ничем не помогает сторонам, связанным договорными обязательствами, желающим провести различие между регистрацией доменов юридическими и физическими лицами, а лишь фиксирует результат этого процесса. Рассматривая возможность создания стандартного элемента данных, регистратуры согласились, что для целей интеграции с возможной будущей системой SSAD, как это было рекомендовано на Фазе 2, возможно, имеет смысл создать стандартизированный способ указания того, входят ли персональные данные в состав регистрационных данных. Хотя мы признаем, что может существовать пример использования, связанный с решениями о раскрытии информации в SSAD, мы бы предпочли отложить такие решения, насколько это уместно, до разработки SSAD, а не предпринимать сейчас шаги, которые могут ограничить полезность этого элемента данных после начала работы SSAD.

Рекомендация заходит гораздо дальше, требуя от ICANN создать это поле в координации с техническим сообществом для использования в EPP и RDDS. Для ясности RySG заявляет о том, что не поддерживает использование этого поля ни в EPP, ни в RDDS. В качестве компромисса мы согласились признать, что это совершенно необязательное поле, которое стороны, связанные договорными обязательствами, решившие провести различие между юридическими и физическими лицами и/или указать, входят ли персональные данные в состав регистрационных данных, могут использовать, но никоим образом не обязаны это делать.

В интересах добросовестного сотрудничества в поисках компромиссного решения регистратуры согласились на создание стандартизированного элемента данных и на то, что стороны, связанные договорными обязательствами, могут, по своему усмотрению, использовать этот стандартный элемент данных. У нас есть большие сомнения по поводу использования такого поля в EPP или RDDS, и мы должны четко заявить, что не поддерживаем его использование ни в одной из этих систем. Мы не услышали убедительного обоснования того, почему такое поле должно использоваться в любом случае, и наша поддержка создания такого поля не является указанием или рекомендацией по его использованию.

V. Подготовленные указания по дифференциации юридических и физических лиц недостаточны

RySG поддерживает концепцию указаний, помогающих сторонам, связанным договорными обязательствами, разобраться в сложных юридических и технических

проблемах, с которыми регистратуры и регистраторы регулярно сталкиваются при ведении бизнеса. По нашему опыту, лучшие указания составляются теми, у кого есть соответствующие знания и интересы, чтобы преодолеть трудности и внести ясность в сложные или неоднозначные вопросы. Несмотря на постоянные возражения и предложения по улучшению, поступившие от сторон, связанных договорными обязательствами, указания по вопросу дифференциации юридических и физических лиц, включенные в настоящий отчет, не соответствуют ни одному из этих критериев.

При разработке указаний, содержащихся в Рекомендации № 2, рабочая группа решила, что это факультативные указания, которые стороны, связанные договорными обязательствами, решившие провести различие между регистрацией доменов юридическими и физическими лицами, могут использовать по своему усмотрению. Однако в формулировке итогового отчета Рекомендация № 2 гласит, что сторонам, связанным договорными обязательствами, решившим провести дифференциацию, СЛЕДУЕТ придерживаться этих указаний. RySG считает, что использование слова СЛЕДУЕТ здесь не совсем точно отражает то, что было согласовано рабочей группой. Согласно RFC 2119, «СЛЕДУЕТ. . . означает, что в определенных обстоятельствах могут существовать веские причины игнорировать конкретный пункт рекомендаций, однако следует понять и тщательно взвесить полный спектр последствий, прежде чем избрать иной образ действия». Поскольку эти указания по дифференциации носят факультативный характер, более подходящим термином здесь является МОЖЕТ («пункт полностью необязателен для выполнения»). Хотя в интересах добросовестного сотрудничества в поисках компромиссного решения регистратуры решили поддержать рекомендацию, необходимо отметить, что мы не согласны с использованием слова СЛЕДУЕТ и что стороны, связанные договорными обязательствами, должны оценить, являются ли эти указания полезными и применимыми для них, прежде чем принимать решение об их принятии.

Короче говоря, указания по вопросу дифференциации юридических и физических лиц, включенные в данный отчет, крайне неадекватны, если их целью является оказание помощи стороне, связанной договорными обязательствами, желающей провести дифференциацию. Указания не достигают цели по нескольким причинам. Во-первых, эти указания сознательно и необоснованно ориентированы на результат. Те, кто выступал за необходимость таких указаний, максимально ограничили процесс дифференциации и связанные с ним юридические требования и соображения. Такой подход является почти намеренной попыткой затушевать, а не преодолеть сложности и риски, связанные с процессом дифференциации, что никак не поможет лицам, получившим эти указания, понять и устранить такие сложности и риски.

Во-вторых, эти указания не представляются целесообразными. Опять-таки, не позволяя справиться с присущими дифференциации сложностями и рисками,

итоговые указания представляют собой не более чем пересказ закона и ожидаемых результатов. Например, в указаниях говорится:

«Регистраторы должны обеспечить четкое информирование о характере и последствиях идентификации владельца домена в качестве юридического лица. Эти сообщения должны включать:

- *Простое и понятное определение юридического лица.*
- *Разъяснение регистратором владельцу домена (субъекту данных) возможных последствий следующих действий:*
 - *Указание на то, что регистрационные данные доменного имени являются данными юридического лица;*
 - *Подтверждение наличия персональных данных или данных, не относящихся к персональным;*
 - *Выражение согласия. Это также соответствует разделу 3.7.7.4 Соглашения об аккредитации регистраторов (RAA)».*

К сожалению, у лиц, которым адресованы эти указания, этот краткий раздел вызывает больше вопросов, чем дает ответов. Что такое юридическое лицо? Что делать, если владелец домена не является субъектом данных? О каких последствиях нужно сообщить субъекту данных? Какие шаги необходимы для обеспечения того, чтобы субъект данных понял эти сообщения (например, A/B-тестирование, пользовательские панели)? Каковы риски в случае невыполнения этих шагов? Как получить осмысленное согласие, особенно в тех случаях, когда владелец домена может не быть субъектом данных? Достаточно ли обучения или уведомления владельца домена для снижения риска? Простое перечисление обязательств, которые в значительной степени уже продиктованы законом, очень мало помогает лицу, получившему эти указания, сориентироваться в этих вопросах.

Аналогичным образом, в самом последнем абзаце указаний говорится следующее:

Проведение различия между владельцами доменов, являющимися юридическими и физическими лицами, само по себе не может быть решающим в вопросе о том, как следует обращаться с информацией (публиковать или скрывать), поскольку данные, предоставленные юридическими лицами, могут содержать персональные данные, защищенные законом о защите данных, например GDPR.

На самом деле это самый сложный и рискованный вопрос в разграничении регистраций юридических и физических лиц. Как EDPB указал ICANN, «[т]от факт, что владелец домена является юридическим лицом, сам по себе не обязательно оправдывает неограниченную публикацию персональных данных, относящихся к

физическим лицам, которые работают в этой организации или представляют ее»⁷³. В данных указаниях ничего не говорится о возможном подходе регистратора к этому вопросу. Рассмотрение этой основной проблемы почти мимоходом серьезно подрывает полезность данных указаний и усиливает нашу озабоченность по поводу общей целесообразности данного совета.

В интересах добросовестного сотрудничества RySG согласилась поддержать публикацию данных указаний, несмотря на вышеизложенные опасения, поскольку в рекомендации четко указано, что указания являются полностью факультативными, и стороны, связанные договорными обязательствами (даже те, которые решили применить дифференцированный подход), никоим образом не обязаны следовать Рекомендации №2. Мы скептически относимся к тому, что эти указания будут широко приняты, не потому, что руководящие указания по данному вопросу нежелательны, а потому, что эти указания не дают ничего для практической реализации и не предлагают никакой поддержки сторонам, которые несут юридические риски.

VI. Заключение

По всем вышеуказанным причинам, учитывая постоянную поддержку различными сторонами в группе по EPDP публикации этого итогового отчета и изложенных в нем рекомендаций, и несмотря на нашу озабоченность в отношении объема рекомендаций, RYSG не возражает против принятия этого отчета и изложенных в нем рекомендаций. Однако следует отметить, что эта поддержка основана на добросовестной вере в то, что все стороны сохраняют согласованный уровень консенсуса. Хотя RySG не поддерживает ряд аспектов этого отчета, руководствуясь духом модели с участием многих заинтересованных сторон и поддерживая ее, мы пошли на компромисс.

⁷³ Письмо EDPB Йорану Марби от июля 2018 года: <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

Заявление меньшинства SSAC относительно окончательного отчета по итогам работы над Фазой 2А ускоренного процесса формирования политики по Временной спецификации для регистрационных данных в gTLD⁷⁴

1 Введение

Консультативный комитет ICANN по безопасности и стабильности (SSAC) высоко оценивает распространение первоначального отчета рабочей группы по итогам ФАЗЫ 2А ускоренного процесса формирования политики (EPDP) по Временной спецификации для регистрационных данных в gTLD (именуемого в дальнейшем «Первоначальный отчет по Фазе 2А EPDP»)⁷⁵ и благодарит рабочую группу за возможность прокомментировать его.

В настоящем документе SSAC предлагает как общие комментарии относительно ускоренного процесса формирования политики в целом, так и конкретные комментарии по отдельным рекомендациям в Первоначальном отчете по Фазе 2А EPDP. SSAC будет рад обсудить эти комментарии с группой по EPDP в удобное для нее время, чтобы разъяснить все непонятные и требующие дополнительного уточнения моменты.

SSAC хотел бы отметить значительное время и усилия, затраченные членами группы по EPDP, и поблагодарить их за вклад в рассмотрение этой важной темы.

2 Историческая справка

В этом разделе мы рассмотрим вопросы, поставленные перед рабочей группой (РГ) на Фазе 2А EPDP, сформулируем несколько замечаний об ускоренном процессе формирования политики в целом, а затем опишем наш подход. В следующем разделе будут представлены наши рекомендации, часть которых относится к общим усилиям, а часть — конкретно к Фазе 2А.

2.1 Вопросы, рассматриваемые РГ на Фазе 2А EPDP

2.1.1 Проведение различия между физическими и юридическими лицами

Общие положения о защите данных (GDPR) обеспечивают особую защиту физических лиц (то есть людей) и не предусматривают защиту юридических лиц

⁷⁴ Документ был опубликован как SAC118 и доступен здесь: <https://www.icann.org/en/system/files/files/sac-118-en.pdf>

⁷⁵ См. «Первоначальный отчет рабочей группы по итогам ФАЗЫ 2А ускоренного процесса формирования политики (EPDP) по Временной спецификации для регистрационных данных в gTLD»: <https://www.icann.org/en/system/files/files/epdp-phase-2a-initial-report-02jun21-en.pdf>

(то есть компаний)^{76,77}. РГ по EPDP уделила этому разграничению большое внимание, особенно на Фазе 2А EPDP. РГ по EPDP рассмотрела, среди прочего, следующие вопросы:

1. Должен ли существовать специальный элемент данных для регистрации того, является ли владелец домена физическим или юридическим лицом?
2. Все ли регистраторы обязаны определять это для каждой регистрации?
3. Какие доказательства необходимы для принятия такого решения?
4. Каковы риски в случае неправильного решения регистратора?
5. Должен ли владелец домена заявлять о том, что является физическим или юридическим лицом, и должен ли регистратор полагаться на это заявление?
6. Должны ли контактные данные владельцев доменов, классифицированных как юридические лица, всегда находиться в открытом доступе?⁷⁸
7. Должны ли контактные данные владельцев доменов, классифицированных как физические лица, быть всегда закрытыми для общего доступа?
8. Должен ли быть общедоступным статус владельца домена?
9. Как следует поступать, если личные данные (PII) физического лица входят в состав регистрационных данных юридического лица?

2.1.2 Возможность индивидуальных контактов

Группе по EPDP было предложено рассмотреть следующие вопросы:

- Имеется ли возможность индивидуальных контактов с использованием единообразного анонимизированного адреса электронной почты, и если да, должно ли это стать требованием?
- Если это осуществимо, но не является требованием, какие указания следует дать связанным с ICANN договорными обязательствами сторонам, желающим применять на практике единообразные анонимизированные адреса электронной почты?

Группа по EPDP отметила, что «индивидуальные контакты» — это расплывчатый термин, и что есть две разные цели, заявленные теми, кто выступает за индивидуальные контакты. Они перечислены ниже: (1) возможность быстро и эффективно связаться с владельцем домена без раскрытия личных данных, и (2) общий идентификатор, который помогает следователям связать регистрации доменов с одним и тем же контактным лицом.

⁷⁶ См. преамбулу 14 GDPR: «Защита, предоставляемая настоящими положениями, должна применяться к физическим лицам, независимо от их гражданства или места жительства, в отношении обработки их персональных данных. Эти положения не распространяются на обработку персональных данных юридических лиц и, в частности, предприятий, созданных как юридические лица, включая наименование и форму юридического лица, а также контактные данные юридического лица». <https://gdpr-info.eu/recitals/no-14/>

⁷⁷ См. статью 4 GDPR: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>

⁷⁸ РГ по EPDP в целом рассматривает процесс запроса и ответа так, как если бы «открытые» данные были опубликованы для всеобщего доступа. Во всех ожидаемых сценариях доступ к регистрационным данным всегда осуществляется через процесс «запрос-ответ». То есть регистрационные данные не публикуются в обычном смысле этого слова. В настоящем документе мы используем выражение «общедоступные» для обозначения данных, которые доступны любому, кто их запросит, без ограничений на использование и без ссылки на источник.

Группа по EPDP попыталась разграничить эти цели, предложив два термина:

- **Контактный адрес электронной почты с привязкой к владельцу домена** — адрес электронной почты для всех доменов, зарегистрированных уникальным владельцем [у данного регистратора] ИЛИ [у разных регистраторов], используемый в качестве псевдонимных данных при обработке сторонами, не связанными договорными обязательствами.
- **Контактный адрес электронной почты с привязкой к регистрации** — отдельный адрес электронной почты однократного применения для каждого доменного имени, зарегистрированного уникальным владельцем, используемый в качестве анонимных данных при обработке сторонами, не связанными договорными обязательствами.

После некоторых размышлений группа по EPDP не дала окончательного ответа о возможности использования адресов электронной почты с привязкой к владельцу домена или регистрации. Группа по EPDP рекомендовала, чтобы «стороны, связанные договорными обязательствами, решившие опубликовать в общедоступной службе каталогов регистрационных данных (RDDS) адрес электронной почты с привязкой к владельцу домена или регистрации, принимали соответствующие меры защиты субъекта данных в соответствии с полученными от органов защиты данных указаниями по методам анонимизации и прилагаемыми юридическими рекомендациями».

SSAC отмечает, что некоторые регистраторы уже внедрили ряд различных методов для поддержки контактного адреса электронной почты, привязанного к владельцу домена. Например, индивидуальные адреса электронной почты с привязкой к каждому владельцу домена создаются и размещаются в домене соответствующего регистратора. Сообщения, отправленные на эти адреса электронной почты, пересылаются регистратором фактическому получателю. Некоторые регистраторы предоставляют веб-форму, с помощью которой можно отправить сообщение владельцу конкретного доменного имени. В большинстве случаев отправитель первоначального сообщения не знает, было ли пересланное сообщение доставлено или открыто. Временная спецификация не содержит требований об уровне обслуживания для пересылки электронной почты^{79,80}.

В настоящее время SSAC не известно ни об одном внедренном решении, которое удовлетворяло бы требованиям к контактному адресу электронной почты, привязанному к регистрации, как определено выше. По некоторым данным было предложено небольшое количество решений, но ни по одному из них не был достигнут консенсус.

⁷⁹ Временная спецификация для регистрационных данных в gTLD, Приложение А. Службы каталогов регистрационных данных, параграф 2. <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

⁸⁰ Существуют документально подтвержденные проблемы с реализованными регистраторами средствами установления контакта. См. стр. 55-59 «Регистрационные данные доменных имен на перепутье: ситуация в ICANN с защитой данных, соблюдением обязательств и возможностью установления контакта». <http://www.interisle.net/domainregistrationdata.html>

2.2 Наблюдения SSAC

Исходя из участия в EPDP, SSAC предлагает два комментария относительно общих усилий по созданию системы дифференцированного доступа, отвечающей многочисленным целям. Под системой дифференцированного доступа SSAC подразумевает систему, которая обеспечивает возможность разного ответа в зависимости от запрашивающего лица и цели запроса. Конкретным примером такой системы является Система обеспечения стандартизованного доступа к закрытым регистрационным данным gTLD и их раскрытия (SSAD).

2.2.1 Конкурирующие интересы

С точки зрения SSAC, при обсуждении политики имеют место три конкурирующих интереса.

1. **Сторонники конфиденциальности.** Некоторые стороны хотят, чтобы контактные данные физических лиц не были общедоступными, за исключением случаев, когда физическое лицо дает явное и информированное согласие на открытый доступ. Они хотят, чтобы эта защита распространялась и на юридических лиц, если их контактные данные содержат PII или если PII могут быть получены на основе контактных данных.
2. **Лица, запрашивающие данные.** Отправители запросов хотят получить максимальное количество данных. Лица, запрашивающие данные, хотят, чтобы защита конфиденциальности была ограничена и максимально приближена к уровню, требуемому по закону. Они хотят, чтобы запросы выполнялись надежно, быстро и недорого.
3. **Контролеры данных**⁸¹. Те, кто собирает и открыто публикует данные, а именно регистраторы и операторы регистратур, хотят минимизировать затраты и риски.

У конкретных лиц или организаций может быть сразу несколько таких конкурирующих интересов.

2.2.2 Невысказанная озабоченность

SSAD — это механизм, предложенный для централизации запросов о предоставлении закрытых регистрационных данных, описанный в рекомендациях 1–18 окончательного отчета по итогам работы над Фазой 2 ускоренного процесса формирования политики (EPDP) GNSO по Временной спецификации для регистрационных данных в gTLD⁸².

⁸¹ Этот термин также охватывает и других лиц, собирающих или обрабатывающих данные, полученные при регистрации (то есть реселлеров).

⁸² См. окончательный отчет по итогам работы над Фазой 2 ускоренного процесса формирования политики по Временной спецификации для регистрационных данных в gTLD:

<https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>

Хорошо продуманная система доступа позволит заявителям с законными потребностями получить доступ к закрытым данным, причем надежно, быстро и недорого.

На данный момент нет уверенности в том, что мы сможем создать удовлетворительную систему дифференцированного контроля доступа. В настоящее время Правление ICANN поручило провести шестимесячную фазу функциональной разработки (ODP), чтобы в результате этой оценки получить информацию для обсуждения рекомендаций по политике. Дата ввода в эксплуатацию предлагаемой SSAD еще не определена. Сообщество раскритиковало первоначальную смету затрат как необоснованно завышенную. Также отсутствует четкое определение того, какие данные и при каких обстоятельствах будут доступны тем, кто их запрашивает. Наконец, стороны, связанные договорными обязательствами, вероятно, проверяют запросы данных вручную, поскольку группа по EPDP не сумела принять решение, в каких случаях возможна автоматизация.

Из-за отсутствия ясности в отношении SSAD некоторые участники EPDP, похоже, считают, что в обозримом будущем они, скорее всего, будут иметь доступ только к общедоступным данным, и настаивают на сохранении минимально необходимой по закону защиты конфиденциальности. Результатом этого является невозможность решить многие вопросы в рамках EPDP.

2.3 Подход SSAC

SSAC считает, что проводящим расследования специалистам по безопасности очень важно получить доступ к регистрационным данным доменных имен. В то же время важно защитить тех, кто имеет на это право. Эти две альтернативы могут сосуществовать. Но они не могут сосуществовать в контексте спора о том, должен ли каждый контакт быть общедоступным или нет в качестве единственного выбора.

Контактная информация, которая считается личной, должна быть конфиденциальной и предоставляться при соответствующих обстоятельствах людям, которые в ней нуждаются. С точки зрения SSAC, своевременная, надежная, эффективная и действенная система дифференцированного доступа позволит достичь результата, который станет улучшением для всех конкурирующих интересов.

Таким образом, по мнению SSAC, внимание сообщества ICANN и корпорации ICANN должно быть сосредоточено на создании и эксплуатации эффективной SSAD.

В настоящее время обсуждение доступа к закрытым данным выходит за рамки Фазы 2А EPDP, а обсуждение отчетов Фазы 1 и Фазы 2 считается закрытым. Поэтому в данном отчете мы даем два вида рекомендаций.

1. Всеобъемлющие рекомендации по дифференцированному доступу и SSAD.

2. В рамках Фазы 2А EPDP мы предлагаем несколько подробных рекомендаций, которые, если они будут приняты, позволят добиться максимума в этой сложной ситуации.

3 Рекомендации

3.1 Рекомендации для GNSO и корпорации ICANN

Рекомендация № 1. SSAC рекомендует Организации поддержки доменов общего пользования (GNSO) и корпорации ICANN сосредоточить свое внимание на создании и эксплуатации эффективной системы дифференцированного доступа.

Необходима система дифференцированного доступа, обладающая следующими свойствами:

Своевременность	Она должна заработать в ближайшее время.
Надежность	Она должна работать предсказуемо и последовательно, как при функционировании системы, так и при принятии решений ее участниками.
Полезность	Она должна давать результаты, которые приносят пользу лицам, запрашивающим данные.
Эффективность	Она должна предоставлять ответы на законные запросы данных быстро и по приемлемой для всех сторон стоимости.
Простота доступа	Процедура получения и сохранения прав доступа должна работать достаточно хорошо, чтобы способствовать, а не препятствовать использованию.

В данном документе термин «эффективная» используется для обозначения системы дифференцированного доступа, отвечающей всем вышеперечисленным требованиям и, разумеется, включающей функциональность, необходимую для управления отдельными запросами и ответами при различных сочетаниях отправителей и целей запросов, как отмечено в разделе 2.2.

3.2 Рекомендации для Фазы 2А EPDP

3.2.1 Проведение различия между физическими и юридическими лицами

С точки зрения специалиста по безопасности, для проведения расследований должно быть доступно максимальное количество регистрационных данных либо через эффективную систему дифференцированного доступа, либо через предоставление открытого доступа в RDDS.

Рекомендация № 2. В отношении проведения различия между юридическими и физическими лицами SSAC рекомендует следующее:

- A. Необходимо определить элемент данных, обозначающий правовой статус владельца домена. Изначально мы предлагаем три допустимых значения: «Физическое лицо», «Юридическое лицо» и «Не указано». «Не указано» будет значением по умолчанию, пока владелец домена не идентифицирует себя как физическое или юридическое лицо. Это поле должно поддерживать значения статуса в зависимости от будущих решений в области политики.
- B. Этот элемент данных должен отображаться в составе общедоступных данных.
- C. Владельцев доменов необходимо относить к категории физических или юридических лиц. Такое требование следует предъявлять во время регистрации всех новых доменов. Для существующих регистраций значение «Не указано» может сохраняться до последующего заполнения этого поля. Регистраторов следует обязать спрашивать в соответствующие моменты, например, при продлении срока регистрации домена и/или при ежегодной проверке достоверности данных, является ли владелец домена физическим или юридическим лицом, с целью в конечном итоге получить эти данные для всех владельцев доменов и сократить количество значений «Не указано» до минимального уровня.
- D. Владельцы доменов в настоящее время могут и должны иметь возможность сделать свои контактные данные общедоступными. Владельцы доменов-юридические лица также должны иметь возможность защиты своих данных с помощью услуг сохранения конфиденциальности и регистрации через доверенных лиц.

Эти рекомендации соответствуют предыдущим рекомендациям SSAC⁸³.

3.2.2 Возможность использования псевдонимных контактных адресов электронной почты

Рекомендация № 3. Относительно возможности использования псевдонимных контактных адресов электронной почты SSAC рекомендует следующее:

- A. Две цели политики — (1) возможность быстро и эффективно связаться с владельцем домена без раскрытия личных данных, и (2) общий идентификатор, который помогает следователям соотнести регистрацию домена с одинаковыми контактами — следует рассматривать обособленно.
- B. Для достижения цели политики (A1) регистраторы должны внедрить (или продолжать использовать) методы поддержки контактного адреса электронной почты, привязанного к владельцу домена (см. раздел 2.1.2, где рассматриваются два метода). Кроме того, SSAC рекомендует разработать единые требования к мерам защиты для контактных адресов электронной почты с привязкой к владельцу домена. Требования должны включать в

⁸³ См. SAC104, раздел 3.6. <https://www.icann.org/en/system/files/files/sac-104-en.pdf>

- себя сохранение конфиденциальности данных владельца домена в соответствующих случаях и обязательства по уровню обслуживания, позволяющие определить ожидания в отношении использования услуги. Эти меры защиты не зависят от выбранного метода (например, уникальные адреса электронной почты или веб-формы).
- С. Для достижения цели политики (A2) необходимы дополнительные исследования методов, их эффективности и компромиссов. При этом мы рекомендуем, *не* определять на Фазе 2A EPDP метод соотнесения регистраций с общим контактным лицом.

Приложение Е. Вклад сообщества

Е.1. Запрос мнений и предложений

В соответствии с руководством по PDP GNSO, на раннем этапе своей деятельности Группа по EPDP была обязана направить каждой группе заинтересованных сторон и группе интересов GNSO официальные просьбы представить заявления. Группе по EPDP также рекомендовалось запросить мнение других организаций поддержки и консультативных комитетов ICANN, у которых могут быть знания, опыт или интерес к рассматриваемому вопросу.

Группа по EPDP запросила информацию по этим двум темам в рамках предложения о раннем участии на фазах 1 и 2, и, соответственно, группа по EPDP рассмотрела и учла предоставленную на тот момент информацию (см. <https://community.icann.org/x/Ag9pBQ> и <https://community.icann.org/x/Ag9pBQ>) в рамках своих дискуссий.

Е.2. Форум общественного обсуждения первоначального отчета

3 июня 2021 года группа по EPDP опубликовала свой [первоначальный отчет для общественного обсуждения](#). В первоначальном отчете излагались размышления группы до этого момента, и он должен был служить инструментом для выяснения мнения сообщества, особенно в тех областях, где сохранялись значительные разногласия. Хотя предварительные рекомендации были включены в первоначальный отчет, группа по EPDP попросила рассмотреть эти рекомендации в совокупности с рядом поставленных вопросов, чтобы способствовать доработке отчета.

Для оптимизации анализа комментариев общественности группа по EPDP воспользовалась формой Google. От групп заинтересованных сторон и групп интересов GNSO, консультативных комитетов ICANN, компаний и организаций поступило шестнадцать комментариев помимо одного комментария от частного лица. Полученные комментарии опубликованы здесь: https://docs.google.com/spreadsheets/d/1aRxF19pd5tEyO07_zaj7YvzOPjflBfgi4WRy-nx8yY/edit?resourcekey#gid=1754667842.

Для оптимизации рассмотрения результатов общественного обсуждения группа по EPDP разработала комплект инструментов анализа комментариев общественности (PCRT) и таблицы обсуждений (см. <https://community.icann.org/x/coMZCg>). Используя онлайн-анализ и работая на пленарных заседаниях, группа по EPDP выполнила анализ и оценку представленных комментариев и согласовала изменения рекомендаций и (или) отчета.

Приложение F. Юридические рекомендации Bird & Bird

Ответ на вопросы 1 и 2 (Дифференциация юридических и физических лиц)

МЕМОРАНДУМ

Кому: Интернет-корпорация по присвоению имен и номеров, группа по EPDP
От кого: Рут Бордман и Фил Брэдли-Шмиг
Дата: 6 апреля 2021 года
Тема: Вопросы касательно юридических лиц, согласия *и пр.*, полученные в марте 2021 года.

Для справки

1. EDPB в [письме Йорану Марби \(июль 2018 года\)](#) указал:

«персональные данные, идентифицирующие отдельных сотрудников (или третьих лиц), действующих от имени владельца домена, не должны быть общедоступными по умолчанию в контексте WHOIS».

Согласие

2. <https://www.icann.org/resources/pages/gtld-registration-data-specs-en/-appendixA> Приложение А к Временной спецификации гласит:

«В ответ на запросы доменного имени Регистратор и Оператор регистратуры ДОЛЖНЫ рассматривать следующие поля как "вымаранные", если только контактное лицо (например, по административным, техническим вопросам) не дало Согласие на опубликование своих контактных данных: (...)».

3. Рекомендация № 6 [итогового отчета по Фазе 1 EPDP](#), принятого Правлением ICANN в мае 2019 года, гласит:

«в минимальный коммерчески приемлемый срок предоставить Владельцу зарегистрированного имени возможность дать Согласие на опубликование вымаранных контактных данных, а также адреса электронной почты, в RDS ответственного регистратора».

4. Кроме того, в сноске 83 [итогового отчета группы по Фазе 2 EPDP](#) от 31 июля 2020 года отмечено:

«Еще одна тема, которая могла бы поспособствовать сокращению ручной обработки — это изучение того, какие юридически допустимые механизмы могли бы реализовать стороны, связанные договорными обязательствами, чтобы позволить субъектам данных во время регистрации доменного имени свободно давать согласие на раскрытие данных либо возражать против раскрытия своих данных. Это упростит обслуживание баз данных с защищенной и незащищенной информацией, открывая незащищенные базы данных для более дешевой автоматизированной обработки».

5. Компания Bird & Bird дала рекомендации по этому вопросу, в частности, в нашем меморандуме от 13 марта 2020 года *«Рекомендации по вариантам согласия для целей публикации персональных данных в RDS и соблюдения требований [GDPR]»* ([«Меморандум о согласии»](#)).

Проведение различий между юридическими и физическими лицами

6. В мае 2019 года Правление ICANN также приняло Рекомендацию № 17 итогового отчета по Фазе 1 EPDP, которая гласит:

«1) Группа по EPDP рекомендует разрешить регистраторам и операторам регистратур проводить различия между владельцами доменов в зависимости от того, являются ли они физическим или юридическими лицами, но не рекомендует вменять им это в обязанность.

2) Группа по EPDP рекомендует корпорации ICANN на основе мандата, разработанного по согласованию с сообществом, как можно скорее выполнить исследование:

- осуществимости дифференцированного подхода к юридическим и физическим лицам и расходов, включая расходы на реализацию и расходы в связи с возможной юридической ответственностью;*
- примеров отраслей или других организаций, где используется дифференцированный подход к юридическим и физическим лицам;*
- рисков для конфиденциальности владельцев зарегистрированных имен, возникающих в связи с дифференцированным подходом к юридическим и физическим лицам; и*
- других потенциальных рисков (если таковые имеются) для регистраторов и регистратур, возникающих в связи с отсутствием дифференцированного подхода.*

3) Группа по EPDP изучит и урегулирует вопрос о проведении различий между физическими и юридическими лицами на Фазе 2».

7. Компания Bird & Bird предоставила рекомендации по данному вопросу, в частности, в следующих документах:
- 7.1 наш меморандум от 25 января 2019 года «*Рекомендации по вопросу ответственности в связи с самоидентификацией владельца домена как физического или юридического лица в соответствии с [GDPR]*» («[Меморандум о дифференциации физических и юридических лиц](#)»); и
 - 7.2 наш меморандум от 9 апреля 2020 года «*Рекомендации по принципу точности данных согласно [GDPR]: уточняющие вопросы по меморандумам "Юридические и физические лица" и "Точность"*» («[Дополнительный меморандум о точности данных](#)»).
8. Участники EPDP, вероятно, также помнят, что в статье 83(2) GDPR перечислены факторы, которые необходимо учитывать, когда надзорный орган принимает решение о необходимости наложения административного штрафа (и определяет его размер). К ним относятся количество затронутых субъектов данных, характер данных, умышленный характер нарушения или халатность, предпринятые контролером действия по уменьшению ущерба и степень ответственности контролера с учетом технических и организационных мер, принятых им в соответствии со статьями 25 и 32 GDPR.
9. На этом фоне вы подняли ряд взаимосвязанных вопросов.

Вопрос 1

Представленный вопрос: Согласно принятой согласованной политике, регистраторы будут предоставлять владельцам доменов возможность дать согласие на публикацию персональных данных, включенных в их регистрационные данные. Пожалуйста, сравните правовые риски для сторон, связанных договорными обязательствами, в следующих обстоятельствах:

1) публикация персональных данных на основании согласия владельца домена, с одной стороны,

и

2) публикация данных на основании (i) самостоятельной идентификации данных владельцем домена как содержащих либо только данные юридического лица, либо также содержащих данные физического лица (организации или физического лица) до публикации и (ii) выполнения процедур проверки, описанных в меморандуме Bird & Bird от 25 января 2019 года (т. е. уведомление/разъяснение; подтверждение; проверка; возможность исправления), с другой стороны.

Анализ

10. Мы предполагаем, что этот вопрос и вопросы ниже касаются сценария, поднятого в качестве проблемы в письме EDPB Йорану Марби в пункте 1 выше;

а именно, когда владелец домена является юридическим лицом, и один из его сотрудников (или представителей), выполняющий регистрацию от имени владельца домена, предоставляет свои собственные персональные данные и/или персональные данные других субъектов данных (например, указывая коллегу в качестве контактного лица по административным вопросам).

11. При таком сценарии последняя из этих двух мер (которую для целей настоящего меморандума мы будем называть «Проверенная самоидентификация», VSC) юридически представляет меньший риск для сторон, связанных договорными обязательствами. Возможна их комбинация.

Согласие

- 11.1 Субъект данных должен сам решить, давать ли согласие. Это означает, что в анализируемом сценарии лицо, осуществляющее регистрацию домена от имени владельца домена (юридического лица), может дать согласие на публикацию только своих персональных данных. Оно не может дать согласие от имени своих коллег или других лиц («сторонние субъекты данных»), если сведения о них предоставлены. В такой ситуации оно может только *передать* стороне, связанной договорными обязательствами, результат решения о согласии, принятого этой третьей стороной.
- 11.2 В этой ситуации, которая, как нам кажется, не является редкостью, первый вариант (полагаться на согласие владельца домена) может привести к тому, что стороны, связанные договорными обязательствами, не смогут конкретно продемонстрировать, что (i) сторонний субъект данных действительно дал согласие; и/или (ii) что такое согласие соответствует всем требованиям GDPR в отношении действительности согласия (которые разъясняются в пунктах 13-18 Меморандума о согласии).
- 11.3 Меморандум о согласии содержит пять вариантов подхода, основанного на согласии (Меморандум о согласии, п. 24). Неясно, какой из этих вариантов предполагается в рамках настоящего вопроса.
- 11.4 Меморандум о согласии содержит следующее разъяснение:
 - 11.4.1 схема, где контролеры запрашивают имеющее силу согласие непосредственно у всех субъектов данных (в противоположность тому, что, по-видимому, предлагается в данном вопросе), приведет к меньшему риску, чем схема, которая опирается только на утверждения владельца домена о том, что имеющее силу согласие было получено от субъектов данных; и
 - 11.4.2 *если*, тем не менее, система построена на подтверждении владельцем домена того, что от субъектов данных было получено имеющее силу согласие, сторонам, связанным договорными обязательствами, лучше либо проверить согласие непосредственно у физических лиц, либо потребовать от владельца домена предоставить *доказательства* того, что имеющее силу согласие было получено.

Проверенная самоидентификация

- 11.5 Второй вариант, указанный в представленном вопросе (VSC), возможно предполагает, что персональные данные, как правило, **не** будут публиковаться в составе регистрационных данных (и на всякий случай, если они будут включены по умолчанию, проводится проверка путем обращения по указанным контактными данным).
- 11.6 Поэтому, *если* какие-либо персональные данные действительно будут включены в состав регистрационных данных, следует надеяться, что это будет редким и непреднамеренным событием⁸⁴. Короче говоря, GDPR по большей части должен быть неприменим, за исключением непреднамеренных пограничных случаев.
- 11.7 В этих теоретически редких исключительных случаях несколько факторов могут смягчить ответственность стороны, связанной договорными обязательствами (особенно в свете статьи 83(2) GDPR, рассмотренной в пункте 8 выше) — будь то неточность или обработка персональных данных без законного основания (например, согласия). В частности:
- 11.7.1 Были предприняты значительные шаги для проверки того, что данные не являются персональными; и
- 11.7.2 Предусмотрен простой способ исправления ошибок.
- 11.8 Одним из аргументов, исходя из прецедентного права Суда ЕС («СЈЕU»), может быть даже то, что в этой ситуации стороны, связанные договорными обязательствами, должны нести ответственность, только если они не смогли должным образом рассмотреть жалобу в отношении данных — то есть только после того, как они будут уведомлены о предполагаемой незаконности и, таким образом, получают возможность «проверить» обоснованность жалобы⁸⁵. Это имеет некоторые параллели с другими режимами ответственности ЕС для операторов онлайн-услуг, которые обрабатывают — невольно — контент, нарушающий законодательство ЕС⁸⁶. Как указано в сноске 88 ниже, это,

⁸⁴ Причиной является ошибка самого владельца домена и/или сбой в механизмах проверки, внедренных стороной, связанной договорными обязательствами.

⁸⁵ В своем решении по делу C-136/17 «GC и другие» CJEU пояснил, что обязательства GDPR, связанные с запросом на удаление данных («право на забвение»), применяются «к оператору поисковой системы в контексте его обязанностей, полномочий и возможностей в качестве контролера обработки, осуществляемой в связи с деятельностью поисковой системы, по случаю проверки, проводимой этим оператором под надзором компетентных национальных органов после получения запроса от субъекта данных». Как пояснил в этом деле Генеральный адвокат, «такой оператор может действовать только в рамках своих обязанностей, полномочий и возможностей». Другими словами, такой оператор может оказаться неспособным обеспечить полное действие положений [закона ЕС о защите данных] именно в силу ограниченности своих обязанностей, полномочий и возможностей. . . Предварительный контроль интернет-страниц, ссылки на которые представлены в результате поиска, не входит в обязанности или возможности поисковой системы». Она не могла знать, с момента индексирования веб-страницы, что содержание страницы (например) устарело (как в первоначальном решении по делу *Google Spain/Costeja*) или (как в деле *GC и другие*) представляет собой данные, относящиеся к «особой категории» или являющиеся элементом «уголовного преступления», для публикации которых требуется согласие.

⁸⁶ Например, см. [статью 14](#) Директивы об электронной торговле 2000/31/ЕС и ее перенос в национальное законодательство стран-членов ЕС/ЕЭЗ и Великобритании.

вероятно, признается в решениях надзорных органов GDPR (по крайней мере, в некоторых).

Сочетание

- 11.9 Хотя вариант VSC обеспечивает меньший риск для сторон, связанных договорными обязательствами, у него есть и обратная сторона: это означает, что персональные данные (как правило) не публикуются. Для некоторых заинтересованных сторон это покажется упущенной возможностью максимизировать доступность открытых регистрационных данных.
- 11.10 Поэтому стороны, связанные договорными обязательствами, возможно, пожелают рассмотреть сочетание механизмов: спросить человека, заполняющего регистрационную форму, предоставляет ли он персональные данные. Если ответ отрицательный, то следует проверить это утверждение, обратившись по указанным контактными данным (VSC). Если ответ положительный, то следует спросить, относятся ли эти персональные данные к этому человеку, и если да, согласен ли он на их публикацию.
- 11.11 Иногда точность представляют как проблему GDPR применительно к публикации регистрационных данных. Хотя наши поиски не выявили существенного прецедента правоприменения в ситуации, аналогичной той, что рассматривается здесь, нам кажется, что при такой комбинированной модели (VSC + согласие):
- 11.11.1 Если владелец домена (или лицо, представляющее его) неправильно охарактеризует персональные данные как не являющиеся персональными, то запущенный в результате этого процесс проверки должен обеспечить разумную защиту сторон, связанных договорными обязательствами, от ответственности за нарушение принципа точности GDPR, как объясняется в пункте 11.7 выше, как и юридический аргумент, изложенный в пункте 11.8 выше.
- 11.11.2 В противном случае, если владелец домена (или лицо, представляющее его) неверно охарактеризует данные, не являющиеся персональными, как персональные, то независимо от того, даст ли он впоследствии согласие на их публикацию, эти данные все равно не будут являться персональными, поэтому ответственность по GDPR не может возникнуть.

ВОПРОС 2

Представленный вопрос: В пунктах с 17 по 25 меморандума компании Bird & Bird от 25 января 2019 года [Меморандум о дифференциации физических и юридических лиц] рассматривались потенциальные риски для регистраторов, связанные с тем, что регистратор полагается на (i) самоидентификацию владельца домена как юридического лица и (ii) подтверждение того, что регистрационные данные не содержат персональных данных. В меморандуме определены различные шаги, которые регистраторы могут предпринять для снижения риска непреднамеренной публикации персональных данных.

Например, в меморандуме предполагалось, что регистраторы могут предпринять определенные шаги для повышения точности самоидентификации/аттестации, такие как: предоставление отдельной, четкой информации, включая описание последствий самоидентификации в качестве юридического лица и просьбу к владельцам доменов подтвердить, что они не предоставляют персональные данные; проверка понятности/читаемости такой информации; периодические последующие электронные письма владельцам доменов и/или контактными лицам по техническим вопросам; предоставление механизма для изменения самоидентификации, исправления или возражения против публикации персональных данных.

Вопрос 2(1): Предполагая, что регистратор примет меры по снижению риска, указанные компанией Bird & Bird, и основываясь на вашем опыте и применимых прецедентах, пожалуйста, опишите уровень риска, вероятность правоприменительных действий, штрафов, разъяснений и так далее, вытекающих из последующей непреднамеренной публикации персональных данных, содержащихся в регистрационных данных юридического лица.

Вопрос 2(2): В продолжение вопроса [2(1)], пожалуйста, опишите уровень рисков (например, правоприменительные действия, штрафы, разъяснения и так далее), с которыми сталкивается сторона, связанная договорными обязательствами, при публикации персональных данных, если в электронном подтверждении, отправленном регистратором владельцу домена и/или контактными лицам по техническим вопросам владельца домена (i) четко указано, что владелец домена сам обозначил себя как юридическое лицо и утвердительно заявил, что персональные данные не были включены в его регистрационные данные; (ii) поясняется, что на основании этих двух заявлений все поля в регистрационных данных будут опубликованы в интернете; и (iii) предоставляется простой в использовании механизм, с помощью которого самоидентификацию можно отменить, а физическое лицо, получившее электронное письмо, может возразить против публикации своих персональных данных и/или исправить любые неточности? Должен ли регистратор требовать от владельца домена и/или контактного лица по техническим вопросам дать утвердительный ответ на электронное письмо-подтверждение? Различается ли ответ в зависимости от способа уведомления (например, физическая почта или электронная почта)?

Вопрос 2(3): Существуют ли дополнительные или альтернативные меры по смягчению последствий и/или проверке, которые сторона, связанная договорными обязательствами, могла бы предпринять для дальнейшего снижения/устранения ответственности, связанной с непреднамеренной публикацией персональных данных в связи с доверием к самоидентификации владельца домена, например, подтверждение существования корпоративных идентификаторов (Inc., GmbH, Ltd. и пр.), проверка данных владельца учетной записи на наличие признаков юридического лица и так далее? В какой степени каждый такой дополнительный шаг уменьшит ответственность?

12. Что касается вопроса 2(1) (уровень риска, в целом, в случае принятия описанных мер VSC): несмотря на поиск прецедентов в нескольких государствах-членах ЕС/ЕЭЗ, нам не известно о сопоставимых прецедентах. Кроме того, обратите внимание, что тенденции правоприменения и политика регулятивных действий постоянно меняются, как и эффективность гражданских исков со стороны истцов.
13. Однако, на наш взгляд, риск для сторон, связанных договорными обязательствами, представляется низким, если они примут меры, описанные в представленном вопросе, чтобы избежать публикации (или, при получении сообщения, сохранения) персональных данных в составе регистрационных данных.
14. Наше мнение основано на следующих факторах (также принимая во внимание статью 83(2) GDPR, рассмотренную в пункте 8 выше):
- 14.1 Ошибочное включение персональных данных, несмотря на описанные там меры (при условии, что они хорошо реализованы), похоже, будет происходить только в исключительных случаях. Как мы советовали в Меморандуме о дифференциации физических и юридических лиц, корпорации ICANN и сторонам, связанным договорными обязательствами, целесообразно проводить исследования (например, собирать статистику), чтобы контролировать, действуют ли меры так, как задумано.
- 14.2 Если персональные данные будут ошибочно включены в опубликованные регистрационные данные, это произойдет, несмотря на существенные (VSC) меры, принятые сторонами, связанными договорными обязательствами, и будет в первую очередь связано с действиями/бездействием владельца домена. Указанное обстоятельство, скорее всего, будет принято во внимание субъектами данных, органами надзора за защитой данных и судами.
- 14.3 Данные, о которых идет речь, скорее всего, имеют низкую конфиденциальность. Предполагаемый здесь сценарий (ошибочное включение персональных данных в опубликованные регистрационные данные), по-видимому, наиболее вероятен, когда юридическое лицо (например, компания или некоммерческая организация) регистрирует/поддерживает свои собственные домены. В этих сценариях мы предполагаем, что персональные данные, которые могут быть раскрыты, обычно относятся к рабочим данным сотрудника (например, адрес электронной почты компании), а не к личной жизни человека. Хотя GDPR обеспечивает защиту даже на рабочем месте, данные, о которых идет речь в данном случае, вероятно, менее способны причинить вред человеку, чем данные, относящиеся к частной жизни субъекта данных⁸⁷.

⁸⁷ Как объяснялось выше, мы понимали этот вопрос как вопрос о сценариях, в которых владельцы доменов являются юридическими лицами, в соответствии с цитатой EDPB в пункте 1. В отношении индивидуальных владельцев доменов (физических лиц) вопросы будут в основном аналогичными: если физическое лицо ошибочно заявит, что его данные не являются персональными данными, то (i) меры проверки должны предотвратить публикацию данных, поскольку они дадут субъекту данных возможность исправить свою ошибку; (ii) смягчающие факторы и юридические аргументы, описанные здесь в пунктах 11.7 и 11.8, а также в

- 14.4 В более деликатных случаях (например, раскрытие информации о том, что человек работает в компании, относящейся к деликатному или «неудобному» сектору), владелец домена подвергает себя серьезному риску жалоб со стороны собственных сотрудников. Таким образом, владельцы доменов заинтересованы в том, чтобы избежать ошибок, которые могут иметь серьезные последствия для их собственного персонала.
- 14.5 Предусмотренные меры включают возможность исправить ошибку. Конечно, природа глобального интернета такова, что может быть трудно полностью удалить ошибочно опубликованные данные из зеркал/кэшей/архивов, если для этого созданы какие-либо службы. Поэтому мы призываем принять дополнительные меры, предусмотренные для вопроса 2(2) ниже.
- 14.6 Наконец, как отмечалось выше, можно на основании дела «GC и другие» привести аргументы, что ответственность должна наступать для стороны, связанной договорными обязательствами, только тогда, когда и если она не сможет должным образом рассмотреть жалобы на включение персональных данных в опубликованные регистрационные данные, а не с более раннего момента непреднамеренной публикации данных. Однако это зависит от того, принял ли контролер разумные меры для предотвращения такого включения (например, меры VSC, рассматриваемые в настоящем документе).

В отношении вопроса 2(2) (уровень риска в случае отправки подтверждения по электронной почте, предлагающего простой способ отмены самоидентификации/исправления неточностей):

15. На наш взгляд, такой метод проверки целесообразен и поможет снизить риск. Это снижение риска будет наиболее значительным при наличии приемлемого льготного периода, в течение которого можно подать возражение, до публикации данных, о которых идет речь, в составе регистрационных данных.
16. Стороны, связанные договорными обязательствами, должны будут учитывать сроки почтовой пересылки («физическая почта»), если используется этот способ — может потребоваться некоторое время, чтобы почта была доставлена в организацию, потом попала к нужному сотруднику (который может отсутствовать в офисе, например, находиться в ежегодном отпуске), а затем была обработана этим лицом. Электронная почта, по крайней мере, обычно не страдает от задержек в доставке; в этом случае льготный период должен учитывать только возможный отпуск и/или временную неспособность получателя работать с электронной почтой по другим причинам.
17. На наш взгляд, требование дать утвердительный ответ на проверочное письмо представляется чрезмерной осторожностью, пока исследования не покажут, что

пунктах 14.1–14.6, должны обеспечить разумную правовую защиту сторон, связанных договорными обязательствами.

- принятые меры не позволяют предотвратить попадание очень значительных объемов персональных данных в опубликованные регистрационные данные. Однако в случае возврата проверочного электронного письма (то есть сторона, связанная договорными обязательствами, знает, что оно не было доставлено) лучше воздержаться от публикации (то есть в данном случае результат проверки VSC следует считать отрицательным).
18. Мы не можем исключить возможность того, что некоторые суды или регулирующие органы придерживаются другого мнения. Даже в этом случае наиболее вероятным представляется предписание устранить проблему (скорее всего, с предоставлением приемлемого срока для внесения изменений), а не штраф, учитывая факторы статьи 83(2) GDPR, рассмотренные в пункте 8 выше. Проведя проверку в ряде государств-членов, мы не нашли соответствующих примеров правоприменения. Соответственно, существует мало указаний, помимо тех, что изложены в самом GDPR.
 19. Что касается вопроса 2(3) (дополнительные или альтернативные шаги для снижения ответственности по VSC): здесь особенно уместны наши рекомендации, изложенные в пунктах 21-25 Дополнительного меморандума о точности. Значительная часть этих комментариев, а также таблица 16 возможных дополнительных мер, которые могут быть приняты для минимизации или компенсации возможных неточностей в регистрационных данных, сохраняют актуальность и здесь.
 20. Вопрос, как вы его поставили, уже повторяет многие из этих мер, а именно: *«предоставление отдельной, четкой информации, включая описание последствий самоидентификации в качестве юридического лица и просьбу к владельцам доменов подтвердить, что они не предоставляют персональные данные; проверка понятности/читаемости такой информации; периодические последующие электронные письма владельцам доменов и/или контактными лицам по техническим вопросам; предоставление механизма для изменения самоидентификации, исправления или возражения против публикации персональных данных»*.
 21. В данном вопросе также предлагается *«подтвердить наличие корпоративных идентификаторов (Inc., GmbH, Ltd. и пр.) [и/или] проверить данные о владельцах учетных записей на наличие признаков юридического лица»*. Кроме того, еще одним способом проверки статуса юридического лица может быть запрос регистрационного номера компании.
 22. Большинство работодателей смогут сообщить регистрационный номер и/или наименование компании, заканчивающееся на Ltd., PLC, SA, BV, GmbH и пр., хотя они также могли предоставить персональные данные о своих сотрудниках, например, контактных лицах для соответствующего домена. Соответственно, такая проверка — даже если она возможна — подтверждает только то, что владелец домена является юридическим лицом. Она не подтверждает, что владельцем домена-юридическим лицом не предоставлены (также) персональные данные, например, о своих сотрудниках. То есть эта мера помогает избежать неправильного описания владельцами доменов-физическими лицами своих собственных данных, но

- это не является серьезным риском (с точки зрения GDPR), поскольку такие лица в любом случае заинтересованы в том, чтобы должным образом заявить о своем статусе физического лица, и их заявление можно проверить, связавшись с ними. На альтернативный и, возможно, более серьезный риск — включение работодателем персональных данных своих сотрудников — такая мера не влияет. Поэтому такая мера приносит ограниченную пользу применительно к GDPR.
23. Полезным, если это возможно, может оказаться технический инструмент, используемый для оценки того, содержат ли адреса электронной почты имя человека или выглядят как адреса общего назначения. Одного этого недостаточно: адреса электронной почты могут быть связаны с идентифицируемым лицом (то есть быть персональными данными), даже если в них не используется его имя. Поэтому такой инструмент следует рассматривать только как часть комплекса мер. Что касается телефонных номеров, в случае их сбора, технический инструмент мог бы использоваться для проверки наличия префиксов номеров сотовой связи (которые обычно привязаны к одному человеку, пожалуй, чаще, чем номера стационарных телефонов).
 24. Такие функции требуют тщательного тестирования, поскольку процент ложноположительных и ложноотрицательных результатов может быть значительным, особенно учитывая международный характер системы доменных имен, работу которой координирует ICANN (даже на английском языке, как мы предполагаем, адреса электронной почты вида «@johndeere.com» или «@annsummers.com» могут представлять трудности).
 25. Вместо того чтобы действовать автоматически на основании результатов, полученных с помощью таких инструментов, возможно, некоторые стороны, связанные договорными обязательствами, будут готовы «вручную» оценивать подозрительные данные, хотя это, вероятно, потребует от сторон, связанных договорными обязательствами, значительных усилий. Кажется более вероятным, что вместо этого такой инструмент будет давать владельцу домена подсказку («*похоже, что вы предоставили контактные данные физического лица, (...)»*) и спрашивать его, хочет ли он игнорировать эту подсказку или принять соответствующие меры.
 26. Поэтому, по сути, такие инструменты лучше использовать как дополнительный (умный, учитывающий содержание) «толчок» для владельцев доменов, а не для автоматического определения возможности опубликовать данные.
 27. Учитывая отсутствие определенности касательно жизнеспособности и достоинств такого подхода, его можно было бы, например, оставить в качестве среднесрочного/долгосрочного пункта для изучения и тестирования; его полную разработку и внедрение можно было бы поставить в зависимость не только от технической осуществимости, но и от определения на основе накопленного опыта реальной необходимости принятия дополнительных мер.

28. Поэтому, в конечном счете, мы пока не можем предполагать, что от сторон, связанных договорными обязательствами, потребуются или ожидаются другие меры, помимо тех, которые уже рассматривались в заданном вопросе.
29. По данному пункту возможны расхождения во мнениях. Кроме того, многое может зависеть от *способа реализации* предложенных мер, в том числе перечисленных в вопросе. Например, в Венгрии существует прецедент, согласно которому, когда точность данных оспаривается, обработка данных (например, публикация) может быть временно приостановлена, за исключением случаев, когда это необходимо для проверки и принятия мер в связи с заявленной неточностью⁸⁸, по-видимому, независимо от того, ссылался ли субъект данных на статью 18(1) GDPR (право требовать ограничения доступа к данным на время проверки сообщений о недостоверности). Хотя предложенная здесь схема, похоже, не требует и не предполагает такой временной приостановки (поскольку субъекты данных смогут незамедлительно самостоятельно исправить самоидентификацию, которую сочтут неточной, то есть сообщение и исправление должны быть, как правило, одновременными событиями), мы рекомендуем иметь это в виду, если планы будут развиваться и в конечном итоге приведут к возможности задержки между отправкой сообщения и исправлением неточных данных.
30. Мы пояснили в Дополнительном меморандуме о точности (пункт 21), что *«ICANN и/или стороны, связанные договорными обязательствами, будут иметь наилучшие возможности для оценки того, являются ли действующие в настоящее время процедуры достаточными или целесообразно принять дополнительные меры для соблюдения Принципа точности, и если да, то оценить, какие меры были бы наиболее уместными»*. В том же меморандуме в пункте 24 говорится, что *«использование статистических данных и мониторинг количества запросов на исправление, поступающих от субъектов данных, также являются мерами, которые могут способствовать обеспечению адекватного уровня точности»*. Например, мониторинг тенденций в запросах на исправление может позволить выявить пробел в точности или определить, где мера может быть не совсем эффективной, и предпринять шаги для устранения пробела или замены меры на более подходящую».

* * *

⁸⁸ Решение NAIH по делу NAIH/2019/363/2: https://www.naih.hu/files/NAIH-2019_363_határozat.pdf; машинный перевод соответствующего отрывка: «Уполномоченный орган соглашается с [ответчиком], что контролер не обязан удалять данные в случае, когда точность данных, ранее предоставленных клиентом, поставлена под сомнение третьей стороной, и не доказано, что данные больше не находятся в распоряжении клиента, а находятся в распоряжении уведомителя. Однако меры, принятые контролером на основании уведомления, должны способствовать соблюдению принципа точности и предотвращать использование неточных данных. Уполномоченный орган считает, что в таком случае контролер должен временно ограничить обработку неточных данных, предприняв разумные шаги».

Ответ на вопрос 3 (Дифференциация юридических и физических лиц)

МЕМОРАНДУМ

Кому: Интернет-корпорация по присвоению имен и номеров, группа по ЕРДР
От кого: Рут Бордман и Фил Брэдли-Шмиг
Дата: 27 апреля 2021 года
Тема: Вопрос (март 2021 года) касательно признания Евросоюзом и третьими сторонами интересов, связанных с публикацией регистрационных данных

Для справки

31. ЕДРВ в письме Йорану Марби («Письмо ЕДРВ от июля 2018 года») ⁸⁹ указывает:

«личные данные, идентифицирующие отдельных сотрудников (или третьих лиц), действующих от имени владельца домена, не должны быть общедоступными по умолчанию в контексте WHOIS».

32. Это вызвало ряд связанных с GDPR вопросов. Они совсем недавно поднимались в нашем меморандуме от 6 апреля 2021 года («**Меморандум о вариантах VSC и согласия**»), где обсуждались два вопроса («**Вопрос 1 и Вопрос 2**») и рассматривались различные подходы (и возникающие риски) в отношении (i) публикации регистрационных данных после получения согласия и (ii) публикации регистрационных данных, если они относятся (только) к юридическому лицу (например, компании) и не являются персональными данными (и возможные способы проверки этого), то есть верифицированная самоидентификация, «VSC».
33. В представленном ниже вопросе вы также интересуетесь, создают ли определенные положения законодательства ЕС и/или практика двух третьих сторон (EURid и RIPE-NCC) полезный прецедент в этой области. В данном меморандуме рассматривается этот третий вопрос.

<p>Представленный вопрос: Регламент Комиссии (ЕС) № 874/2004 от 28 апреля 2004 года, устанавливающий правила общественной политики в области внедрения и функций домена верхнего уровня .eu и принципы, регулирующие регистрацию («Регламент работы .eu»), устанавливает правила общественной политики, касающиеся внедрения и функций домена верхнего уровня .eu (TLD) и принципы общественной политики в области регистрации доменных имен в TLD .eu.</p>
--

⁸⁹ Письмо ЕДРВ Йорану Марби от 5 июля 2018 года:
https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf

Статья 16 Регламента работы .eu называется «База данных WHOIS» и гласит:

«Целью базы данных WHOIS является предоставление достаточно точной и актуальной информации о контактных лицах по техническим и административным вопросам, управляющих доменными именами в TLD .eu.

База данных WHOIS должна содержать информацию о владельце доменного имени, которая является релевантной и не избыточной по отношению к назначению базы данных. Если информация не является строго необходимой по отношению к назначению базы данных и при этом владелец доменного имени является физическим лицом, то для публикации такой информации необходимо получить однозначное согласие со стороны владельца доменного имени. Преднамеренное предоставление неточной информации является основанием для признания регистрации доменного имени нарушающей условия регистрации».

С 13 октября 2022 года Регламент работы .eu будет упразднен из-за вступления в силу Регламента 2019/517, где в статье 12 «База данных WHOIS» сказано:

«1. Регистратура должна создать базу данных WHOIS и управлять ей с должной тщательностью с целью обеспечения безопасности, стабильности и устойчивости TLD .eu путем предоставления точной и актуальной регистрационной информации о доменных именах в TLD .eu.

2. База данных WHOIS должна содержать релевантную информацию о контактных лицах, управляющих доменными именами в TLD .eu, и о владельцах доменных имен. Информация в базе данных WHOIS не должна быть избыточной по отношению к назначению базы данных. Регистратура должна соответствовать Регламенту (ЕС) 2016/679 Европейского парламента и Совета».

В настоящее время база данных WHOIS находится в ведении EURid, некоммерческой организации, назначенной Европейской комиссией для управления регистратурой .eu. В своей базе данных WHOIS компания EURid публикует адреса электронной почты владельцев доменных имен в TLD .eu (как физических, так и юридических лиц). EURid проводит различие между физическими и юридическими лицами, публикуя информацию о почтовом адресе юридических лиц, в то время как для физических лиц эта информация не публикуется.

Благодаря статье 16 Регламента работы .eu EURid может опираться на статью 6(1)(e) GDPR, которая обеспечивает правовую основу для обработки персональных данных, необходимых для выполнения задачи, решаемой в общественных интересах или в рамках осуществления официальных полномочий, возложенных на контролера. Хотя мы понимаем, что это основание с точки зрения общественных интересов, предусмотренное статьей 16,

недоступно за пределами домена .eu, существование такого законного основания для обработки данных EURid может быть истолковано как предположение, что законодательный орган ЕС признал, что раскрытие данных владельцев доменов служит законным интересам стабильности, безопасности и устойчивости. Кроме того, реализуя свои полномочия в соответствии со статьей 16, EURid определил, что публикация электронной почты владельца домена «не является чрезмерной по отношению к назначению базы данных».

Аналогичным образом, хотя RIPE-NCC полагается на согласие для публикации личной информации о контактных лицах по техническим и административным вопросам, он публикует личную информацию о владельцах ресурсов на том основании, что «содействие координации между сетевыми операторами является единственной целью, которая оправдывает публикацию персональных данных в базе данных RIPE-NCC, и очевидно, что обработка персональных данных, относящихся к владельцу ресурса, необходима для выполнения функций регистратуры, которая осуществляется в законных интересах сообщества RIPE и бесперебойной работы интернета во всем мире (и поэтому соответствует статье 6.1.f GDPR)».

Мы понимаем, что основание с точки зрения общественных интересов, предусмотренное статьей 16, недоступно сторонам, связанным договорными обязательствами, за пределами домена верхнего уровня .eu. Исходя из вашего опыта и применимых прецедентов, в какой степени (если таковые имеются): (i) существование статьи 16 Регламента ЕС; (ii) решение EURid о публикации адресов электронной почты владельцев доменов в соответствии со статьей 16; (iii) решение RIPE-NCC о публикации адресов электронной почты владельцев ресурсов; и (iv) проект формулировки о доступе к регистрационным данным в недавно предложенной Директиве NIS2 создают прецедент, который снизит риск стороны, связанной договорными обязательствами, в связи с публикацией адреса электронной почты владельца домена-юридического лица, даже если он содержит личную информацию? Влияют ли эти факты на ваши ответы на вопросы [1-2]? Если это не влияет на ваши ответы, пожалуйста, объясните почему.

34. Мы считаем, что в целом цитируемые документы не влияют на наши ответы на вопросы 1 и 2 в Меморандуме о VSC и вариантах согласия. Говоря более конкретно, мы считаем, что цитируемые документы имеют ограниченное влияние на риск стороны, связанной договорными обязательствами, в связи с публикацией адреса электронной почты владельца домена-юридического лица, даже если он содержит персональные данные. Наше мнение основано на причинах, изложенных ниже.

Регламент (ЕС) 2019/517, заменяющий Регламент Комиссии (ЕС) № 874/2004 («Новый регламент работы .EU»)

35. Когда Регламент (ЕС) 2019/517 («Новый регламент работы .EU») заменит Регламент Комиссии (ЕС) № 874/2004 («Старый регламент работы .EU»), он аннулирует положение Старого регламента работы .EU, которое разрешало

- «не являющуюся строго необходимой» публикацию персональных данных в составе регистрационных данных (если субъект данных дал на это явное согласие). Соответствующие положения цитируются в представленном вопросе.
36. В Новом регламенте работы .EU не сказано прямо, что подход, основанный на согласии, оказался непрактичным или не соответствующим требованиям; там просто нет никаких комментариев по поводу такого подхода. На самом деле, в новом Регламенте работы .EU не содержится никаких комментариев о публикации персональных данных, будь то «строго необходимая» или иная. Он ограничивается требованием, чтобы обработка данных соответствовала GDPR (если применимо), не указывая, каким образом. В частности, пункт 22 Регламента (ЕС) 2019/517 требует от регистратуры .eu выбрать такую реализацию базы данных WHOIS и связанных с ней систем, которая соответствует требованиям о «защите персональных данных по замыслу и по умолчанию», «необходимости» и «пропорциональности».
37. Наиболее прямое упоминание о распространении регистрационных данных, если это персональные данные, можно найти в преамбуле 21. Здесь говорится только о раскрытии данных/доступе к ним *правоохранительных органов*, действующих в соответствии с «[законодательством ЕС] или национальным законодательством», но *не* широкой общественности и *не* заинтересованных сторон, таких как правообладатели интеллектуальной собственности⁹⁰:
- «21. Регистратура должна поддерживать правоохранительные органы в борьбе с преступностью путем реализации технических и организационных мер, направленных на обеспечение доступа компетентных органов к данным, содержащимся в регистратуре, в целях предотвращения, выявления, расследования и пресечения преступлений, как это предусмотрено законодательством Союза или страны».
38. По сути, Новый регламент работы .EU занимает здесь преимущественно нейтральную и неоднозначную позицию. Он в целом отстает от требований GDPR, и *в частности* указывает на необходимость соблюдения пропорциональности и конфиденциальности по умолчанию. Тот факт, что в нем рассматривается законный доступ *конкретных* групп заинтересованных лиц, не обязательно исключает систему, в которой некоторые персональные данные становятся общедоступными, например, с согласия субъекта данных. Тем не менее, из Нового регламента работы .EU исключена формулировка (присутствовавшая в предыдущем), которая явно признавала подход, основанный (частично) на согласии; возможно, что надзорный орган или суд может попытаться сделать из этого неблагоприятный вывод.

⁹⁰ В других упоминаниях о более широком круге заинтересованных сторон не говорится о предоставлении им данных владельцев доменов. Например, в преамбуле 20 говорится: «Регистратура должна принять четкую политику, направленную на своевременное выявление неправомерных регистраций доменных имен и, при необходимости, сотрудничать с компетентными органами и другими государственными органами, имеющими отношение к кибербезопасности и информационной безопасности, которые конкретно участвуют в борьбе с такими регистрациями, например, с национальными группами реагирования на инциденты информационной безопасности (CERT)». «Сотрудничество» *может* повлечь за собой раскрытие персональных данных, но (возможно, намеренно) в Новом регламенте работы .EU ничего об этом не сказано.

Использование EURid правовой основы GDPR «выполнение задачи в общественных интересах»

39. Поставленный вопрос предполагает, что EURid опирается на статью 16 Старого регламента работы .EU, утверждая, что (частичная) публикация персональных данных владельцев доменов разрешена статьей 6(1)(e) GDPR.
40. Статья 6(1)(e) GDPR разрешает обработку, которая требуется для выполнения задачи в общественных интересах или при исполнении официальных полномочий, которыми наделен контролер. Эти положения должны быть закреплены в законодательстве ЕС или государства-члена ЕС.
41. Если сформулированное в вопросе предположение верно⁹¹, то EURid косвенно утверждает, что такая публикация «строго необходима в связи с назначением базы данных». Если бы это было не так, то EURid действовал бы в нарушение статьи 16 Старого регламента работы .EU, поскольку в ней говорится, что «если информация не является строго необходимой по отношению к назначению базы данных и при этом владелец доменного имени является физическим лицом, то для публикации такой информации необходимо получить однозначное согласие со стороны владельца доменного имени». Исходя из формулировки вопроса, насколько мы понимаем, EURid не получает такого согласия.
42. С одной стороны, эта предполагаемая позиция указывает на то, что по крайней мере одна регистратура (EURid) признает важность («строгую необходимость») публикации (некоторых) данных в WHOIS, даже если это персональные данные, и без согласия, или таких мер, как VSC (при условии, по крайней мере, что часть персональных данных вымарывается, согласно политике EURid по данному вопросу)⁹².
43. Однако мнение, которого придерживается EURid, не обязательно отражает точку зрения судов или надзорных органов, обеспечивающих соблюдение GDPR, и не является для них обязательным. Это мнение одной из множества

⁹¹ Мы не смогли подтвердить это; в текущем [уведомлении EURid о конфиденциальности](#) не указано, какая правовая основа GDPR оправдывает публикацию регистрационных данных, хотя там говорится: «Мы обязаны поддерживать полную и точную базу данных всех зарегистрированных доменных имен». Назначением средства поиска WHOIS (<https://whois.eurid.eu/en/>) является предоставление точной и актуальной информации о контактных лицах по техническим и административным вопросам, управляющих доменными именами. Это помогает нам в создании и сохранении надежной и безопасной среды интернета». Ссылка на то, что публикации «необходимы», по-видимому, соответствует либо статье 6(1)(e) GDPR (выполнение задачи в общественных интересах), либо статье 6(1)(c) (юридическое обязательство).

⁹² Мы с интересом отмечаем, что в заданном вопросе утверждается, что EURid ссылается на статью 6(1)(e) GDPR — выполнение задачи в общественных интересах/в интересах государственных органов, а не на статью 6(1)(f) GDPR (законные интересы). EURid не является государственным органом, поэтому в принципе может ссылаться на законные интересы при публикации персональных данных. Мы не осведомлены о причинах, по которым EURid избегает использовать в качестве основания «законные интересы», и поэтому не можем предложить содержательный комментарий по этому наблюдению; тем не менее, используемое основание может оказаться бесполезным/неудовлетворительным для других сторон, связанных договорными обязательствами; в отличие от EURid, большинство сторон, связанных договорными обязательствами, не могут полагаться на статью 6(1)(e) GDPR, поскольку, в отличие от EURid, не существует законов ЕС или государства-члена, лежащих в основе их собственной обработки данных, связанных с WHOIS.

- регистратур. Тот факт, что политику этой конкретной регистратуры тоже контролирует Европейская комиссия⁹³, имеет столь же ограниченное прецедентное значение; даже если — гипотетически — EURid и Европейской комиссией обсуждали совместно этот вопрос, последняя не обеспечивает соблюдение GDPR и не выступает от имени тех, кто этим занимается.
44. В представленном вопросе также сказано, что «EURid проводит различие между физическими и юридическими лицами, публикуя информацию о почтовом адресе юридических лиц, в то время как для физических лиц эта информация не публикуется». Действующая [Политика регистрации EURid \(ред. 11\)](#) содержит следующее разъяснение: «Если наименование предприятия или организации не указано, владельцем домена считается физическое лицо, запрашивающее регистрацию доменного имени; если наименование предприятия или организации указано, то владельцем домена считается предприятие или организация».
45. Это может означать предположение о том, что предоставленные организацией (владельцем домена-юридическим лицом) почтовые реквизиты *не* содержат персональных данных; или просто, что эти данные публикуются как строго необходимые и/или риск для физических лиц снижен. EURid — как контролер большей части данных, о которых идет речь, — будет иметь больше возможностей, чем мы, чтобы на практике определить, соответствует ли это предположение действительности.
46. Даже если это предположение гипотетически справедливо для EURid и почтовых адресов, которые он публикует в составе регистрационных данных юридических лиц в зоне .eu, мы отмечаем, что в свете комментариев EDPB, полученных ICANN⁹⁴, представляется нецелесообразным экстраполировать это на другую контактную информацию (например, адреса электронной почты, которые могут относиться конкретно к одному легко идентифицируемому лицу в организации).
47. На основании этих замечаний, а также с учетом того, что EURid действует в рамках довольно уникальной законодательной базы, дающей ему возможность полагаться на нечто иное, чем согласие или законные интересы, — в отличие от других сторон, связанных договорными обязательствами, — трудно сделать какие-либо общие выводы из подхода EURid.

⁹³ Например, положение 11 Нового регламента работы .EU гласит: «Комиссия должна заключить договор с назначенной регистратурой, содержащий подробно изложенные принципы и процедуры, применяемые к регистратуре для организации, администрирования и управления TLD .eu».

⁹⁴ «Тот факт, что владелец домена является юридическим лицом, сам по себе не обязательно оправдывает неограниченную публикацию персональных данных, относящихся к физическим лицам, которые работают в этой организации или представляют ее, например физическим лицам, которые решают административные или технические вопросы от имени владельца домена». Например, публикация личного адреса электронной почты контактного лица по техническим вопросам, состоящего из имя.фамилия@компания.com, может раскрыть информацию о его текущем работодателе, а также о его роли в организации. Наряду с адресом владельца домена это может раскрывать информацию о месте его/ее работы». Письмо EDPB от июля 2018 года, стр. 5.

Решение RIPE-NCC о публикации адресов электронной почты владельцев ресурсов

48. В вопросе цитируется опубликованная в 2018 году заметка в блоге, автором которой является руководитель юридического отдела RIPE-NCC, озаглавленная [«Как мы внедряем GDPR: правовые основания для законной обработки персональных данных и база данных RIPE»](#).
49. В этой заметке, как правильно указано в заданном вопросе, RIPE-NCC заявляет, что опирается на законные интересы (правовое основание, сформулированное в ст. 6(1)(f) GDPR) для публикации персональных данных — в первую очередь контактной информации — с целью содействия надлежащему функционированию важной интернет-системы.
50. Однако следует отметить, что в этой заметке также сказано:
- «Однако, когда владелец ресурса назначает другое лицо для выполнения этой роли [то есть роли контактного лица], он должен получить согласие лица (лиц), чьи персональные данные будут внесены в Базу данных RIPE, прежде чем их данные будут внесены (в соответствии со статьей 6.1.a GDPR)».
51. Другими словами, нам представляется, что когда владелец ресурса является юридическим лицом, (i) RIPE-NCC считает законные интересы надлежащей правовой основой для первой стороны (то есть когда лицо, выполняющее/обновляющее регистрацию, предоставляет свои собственные контактные данные и, следовательно, является соответствующим субъектом данных), но (ii) RIPE-NCC (по крайней мере, в 2018 году) предпочитает делать это только с согласия субъекта данных для третьей стороны (например, когда контактные данные принадлежат коллеге лица, выполняющего/обновляющего регистрацию).
52. Такое разграничение может быть вызвано опасениями, что будет сложнее утверждать, что собственные интересы третьей стороны в достаточной степени совпадают с интересами владельца ресурса и/или RIPE-NCC (и связанных с ними заинтересованных сторон); и/или опасениями, что существуют более существенные риски для сторонних субъектов данных (например, потому что им сложнее направить уведомление о конфиденциальности GDPR, поэтому они могут быть хуже осведомлены о своих правах). Соответственно, такие опасения могли побудить RIPE-NCC полагаться на согласие в ситуациях с «третьей стороной».
53. Хотя RIPE-NCC должен самостоятельно обратиться за юридическими рекомендациями по этому вопросу, по нашему мнению, как и по мнению ICANN-EPDP, в законодательстве отсутствует требование о таком разграничении. Статья 6(1)(f) GDPR (основание «законные интересы») не требует, чтобы интересы субъекта данных совпадали с интересами контролера. Просто необходим надлежащий *баланс* между интересами (контролера и/или третьих сторон) и «основными правами и свободами субъекта данных, которые требуют защиты персональных данных». В этом случае RIPE-NCC и его собственные юристы будут иметь наилучшее представление о различных интересах и рисках, однако нам представляется, что:

- 53.1 Интересы контролера и более широкого круга заинтересованных сторон, по-видимому, в целом одинаковы, если речь идет о контактных данных первой или третьей стороны: например, любой набор контактных данных предположительно важен для надлежащего расследования и устранения сбоев в работе ключевой интернет-системы.
- 53.2 Что касается рисков, то контактные данные первой или третьей стороны в равной степени могут быть использованы не по назначению, например, для нежелательной рекламной деятельности; могут быть и другие виды рисков, но, опять же, они, скорее всего, будут одинаковыми для субъектов данных как первой, так и третьей стороны.
- 53.3 Что касается вопроса об уведомлении, в GDPR прямо признается возможность ситуаций, когда данные не получены непосредственно от субъекта данных и поэтому невозможно направить уведомление (см., в частности, статью 14(5) GDPR). То есть это не является поводом непременно отказаться от возможности использовать в качестве основания законные интересы в контексте третьих лиц.
- 53.4 Возможно, именно по этой причине в письме, полученном ICANN от EDPB в июле 2018 года, была одобрена возможность использования законных интересов в качестве основания даже для данных третьих сторон при условии, что владельцы доменов не принуждают предоставлять такие данные третьих сторон, а вместо этого они могут предоставить свои собственные⁹⁵. Мы понимаем, что это действительно так для системы, контролируемой RIPE-NCC.
54. Вероятно, RIPE-NCC считает, что регулирующие органы и суды будут априорно приветствовать самостоятельность и контроль, предлагаемые получением согласия, в отличие от правового основания GDPR, не предполагающего получение согласия, такого как законные интересы. Однако эти органы также могут признать практические недостатки такого подхода:
- 54.1 В самой заметке RIPE-NCC признаются сомнения, которые иногда связаны с получением согласия в контексте трудовых отношений (то есть, такое согласие, если оно запрошено работодателем, возможно, не было дано работником добровольно).
- 54.2 RIPE-NCC также полагается на заявления первой стороны о том, что от третьей стороны получено имеющее силу согласие («RIPE NCC считает, что ответственность за получение имеющего силу согласия на обработку лежит на том, кто внес данные в базу данных RIPE (то есть на персонале сопровождения)»). Теоретически это может затруднить для RIPE-NCC (как контролера) демонстрацию того, что эти согласия соответствуют всем требованиям GDPR.

⁹⁵ Письмо EDPB от июля 2018 года, стр. 2-3.

- 54.3 Стороны, связанные договорными обязательствами, могут столкнуться с теми же проблемами GDPR в отношении регистрационных данных доменных имен.
55. Мнение RIPE-NCC, как и мнение EURid, не обязательно отражает мнение органов власти, которым поручено обеспечение соблюдения GDPR и уж точно не является обязательным для исполнения.
56. Более того, процедура уравнивания законных интересов, которую должен провести RIPE-NCC, отличается от процедуры ICANN и сторон, связанных договорными обязательствами; данные, о которых идет речь, относятся к разным ресурсам (ресурсы IPv4, IPv6 и номера автономных систем, которые RIPE-NCC часто выделяет блоками очень крупным организациям, в отличие от конкретных доменных имен, иногда регистрируемых конкретными физическими лицами для частного использования).
57. Поэтому из подхода RIPE-NCC трудно сделать какие-либо общие выводы.

Проект формулировки относительно доступа к регистрационным данным в недавно предложенной Директиве NIS2

58. В декабре 2020 года Европейская комиссия опубликовала проект [уточненной редакции Директивы о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем \(NIS2\)](#).
59. Положения предлагаемой Директивы NIS2 гласят:

«15. Поддержка и сохранение надежной, отказоустойчивой и защищенной системы доменных имен (DNS) — ключевой элемент усилий по обеспечению целостности интернета, и он критически важен для его бесперебойной и стабильной работы, от которой зависят цифровая экономика и общество. Следовательно, действие Директивы должно распространяться на всех провайдеров услуг DNS в цепочке разрешения DNS, в том числе на операторов корневых DNS-серверов, DNS-серверов доменов верхнего уровня, авторитативных серверов доменных имен и рекурсивных резолверов.

(...)

(59) Поддержка достоверных и полных баз данных доменных имен и регистрационных данных (так называемых «данных WHOIS») и предоставление законного доступа к этим данным критически важны для обеспечения безопасности, стабильности и отказоустойчивости DNS, что, в свою очередь, способствует повышению общего уровня кибербезопасности в странах Евросоюза. Если обработка охватывает персональные данные, она должна соответствовать законодательству Евросоюза о защите данных.

(60) Наличие этих данных и возможность своевременного доступа к ним государственных органов, включая компетентные органы в соответствии с законодательством Евросоюза или страны, для предотвращения, расследования или пресечения уголовных преступлений, групп CERT (CSIRT), а в отношении данных их клиентов — поставщиков сетей и услуг

электронной связи и поставщиков технологий и услуг кибербезопасности, действующих от имени этих клиентов, имеет важное значение для предотвращения злоупотреблений в системе доменных имен и борьбы с ними, в частности, для предотвращения, обнаружения и реагирования на инциденты кибербезопасности. Такой доступ должен соответствовать законодательству Евросоюза о защите данных в той мере, в какой он связан с персональными данными.

(61) Для обеспечения доступности точных и полных регистрационных данных доменных имен регистратуры TLD и организации, предоставляющие услуги регистрации доменных имен в TLD (так называемые регистраторы), должны собирать и гарантировать целостность и наличие регистрационных данных доменных имен. В частности, регистратуры TLD и организации, предоставляющие услуги регистрации доменных имен для TLD, должны установить политику и процедуры для сбора и поддержания точных и полных регистрационных данных, а также для предотвращения и исправления неточных регистрационных данных в соответствии с правилами защиты данных Евросоюза.

(62) Регистратуры TLD и организации, предоставляющие для них услуги по регистрации доменных имен, должны сделать общедоступными (так в оригинале) регистрационные данные доменных имен, не подпадающие под действие правил защиты данных Евросоюза, например, данные, касающиеся юридических лиц. Регистратуры TLD и организации, предоставляющие услуги по регистрации доменных имен для TLD, должны также предоставлять законный доступ к конкретным регистрационным данным доменных имен, касающимся физических лиц, лицам, запрашивающим доступ на законных основаниях, в соответствии с законодательством Евросоюза о защите данных. Государства-члены должны обеспечить, чтобы регистратуры TLD и организации, предоставляющие для них услуги по регистрации доменных имен, без неоправданной задержки отвечали на запросы о раскрытии регистрационных данных доменных имен лицам, запрашивающим доступ на законных основаниях. Регистратуры TLD и организации, предоставляющие для них услуги по регистрации доменных имен, должны установить политику и процедуры для публикации и раскрытия регистрационных данных, включая соглашения об уровне обслуживания для рассмотрения запросов на доступ от лиц, запрашивающих доступ на законных основаниях. Процедура доступа может также включать использование интерфейса, портала или другого технического средства для создания эффективной системы отправки запросов и получения доступа к регистрационным данным. С целью продвижения согласованной практики на внутреннем рынке, Комиссия может принять руководящие принципы по таким процедурам без ущерба для компетенции Европейского совета по защите данных.

(...)

69. Обработка персональных данных в строго необходимой и соразмерной степени для целей обеспечения сетевой и информационной безопасности организациями, государственными органами, группами CERT, CSIRT и поставщиками технологий и услуг безопасности должна представлять собой

- законный интерес соответствующего контролера данных, как указано в Регламенте (ЕС) 2016/679. Это должно включать меры, связанные с предотвращением, обнаружением, анализом и реагированием на инциденты, меры по повышению осведомленности о конкретных киберугрозах, обмен информацией в контексте устранения уязвимостей и скоординированного раскрытия информации, добровольный обмен информацией об этих инцидентах, а также о киберугрозах и уязвимостях, индикаторах компрометации, тактике, методах и процедурах, предупреждениях систем кибербезопасности и средствах конфигурирования. Такие меры могут потребовать обработки следующих типов персональных данных: IP-адреса, унифицированные адреса ресурсов (URL), доменные имена и адреса электронной почты».
60. Преамбулы 59-62 включительно в целом также отражены в статье 23 проекта Директивы NIS2.
61. Преамбулы 15, 59-61 включительно и 69, а также статьи 23(1-3) проекта Директивы NIS2 широко поддерживают полную, всестороннюю обработку регистрационных данных, если она соответствует требованиям GDPR. Заключительное предложение преамбулы 61 также прямо поддерживает меры, направленные на содействие соблюдению принципа точности GDPR, например те, которые упоминались в наших предыдущих меморандумах.
62. Однако преамбула 62 и статьи 23(4-5) имеют более конкретное отношение к вопросам, обсуждаемым в данном меморандуме, поскольку касаются публикации/распространения регистрационных данных, а не только их сбора и хранения. Эти положения Директивы NIS2 проводят четкое различие между персональными и прочими данными и прямо поддерживают только публикацию данных, не относящихся к персональным. В отношении персональных данных Директива NIS2 ограничивается рассмотрением того, что представляется как *ограниченный доступ* «лиц, запрашивающих доступ на законных основаниях, в соответствии с законодательством Союза о защите данных» (и эквивалентной формулировкой в статье 23(5)).
63. Поэтому, на наш взгляд, в текущем проекте Директивы NIS2 не рассматривается система, в которой некоторые персональные данные могут открыто публиковаться (на законных основаниях), например, с согласия владельца домена. Неясно, произошло ли это только потому, что такой вариант не рассматривался составителями, *или* потому, что составители не сочли такой подход целесообразным и/или соответствующим требованиям. Однако это означает, что текущий проект Директивы NIS2 не предлагает значительной поддержки/снижения рисков для системы, основанной, например, на согласии владельца домена (хотя и не подрывает такой подход).

* * *

Ответ на вопрос 4 (относительно вариантов маскировки контактных адресов)

МЕМОРАНДУМ

Кому: Интернет-корпорация по присвоению имен и номеров, группа по EPDP
От кого: Рут Бордман и Фил Брэдли-Шмиг
Дата: 9 апреля 2021 года
Тема: Вопрос (март 2021 года) относительно вариантов маскировки контактных адресов

Для справки

64. Европейский совет по защите данных (EDPB) в [письме Йорану Марби \(июль 2018 года\)](#) сообщил:

«персональные данные, идентифицирующие отдельных сотрудников (или третьих лиц), действующих от имени владельца домена, не должны быть общедоступными по умолчанию в контексте WHOIS».

65. Ввиду вышеизложенного и с учетом полученных вами предыдущих рекомендаций по этому вопросу, вы задали следующий вопрос.

Представленный вопрос: В подготовленном В&В [меморандуме от 4 февраля 2020 года относительно информации по контактным адресам электронной почты](#) рассматривались два варианта: (а) «псевдонимный контактный адрес электронной почты», когда одна и та же уникальная строка используется для нескольких регистраций субъекта данных; и (b) «анонимный контактный адрес электронной почты», когда для каждой такой регистрации используется отдельная уникальная строка электронного адреса. Компания В&В высказала мнение, что публикация (а) или (b) будет рассматриваться как публикация персональных данных в интернете, поскольку цель предоставления маскированного адреса электронной почты — позволить третьим лицам напрямую связаться с субъектом данных, и поскольку третьи лица с законными и соразмерными интересами будут иметь доступ к базовым данным.

По результатам рассмотрения Юридический комитет группы по EPDP предложил в дальнейшем описать варианты (а) и (b) следующим образом:

- Фразу «псевдонимный контактный адрес электронной почты» (вариант (а)) следует заменить фразой «**контактный адрес электронной почты с привязкой к владельцу домена**», определяемый как: «адрес электронной почты для всех доменов, зарегистрированных уникальным владельцем домена, *используемый в качестве псевдонимных данных при обработке*

сторонними пользователями (то есть сторонами, не связанными договорными обязательствами). (Для ответа на вопрос о том, должен ли этот адрес электронной почты быть общим для всех регистраторов, аккредитованных ICANN, необходимо выработать соответствующую политику.)

- Фразу «анонимный контактный адрес электронной почты» (вариант (b)) следует заменить фразой **«контактный адрес электронной почты с привязкой к регистрации»**, определяемый как «отдельный адрес электронной почты однократного применения для каждого доменного имени, зарегистрированного уникальным владельцем, *используемый в качестве практически или «по сути» анонимных данных при обработке сторонними пользователями* (то есть сторонами, связанными договорными обязательствами)».

Отвечая на приведенные ниже вопросы, пожалуйста, в целях обсуждения исходите из предположения, что сторонние пользователи информации о контактных адресах электронной почты с привязкой к регистрации не могут идентифицировать субъекта данных без несоразмерных усилий, так что риск идентификации в действительности представляется незначительным.

1. Исходя из вашего опыта и применимых прецедентов, сравните уровень риска, вероятность правоприменительных действий, штрафов, консультаций и так далее, связанных с (a) публикацией в интернете или (b) автоматическим раскрытием (i) контактного адреса электронной почты с привязкой к владельцу домена, с одной стороны, и (ii) контактного адреса электронной почты с привязкой к регистрации, с другой стороны.

Отвечая на этот вопрос, пожалуйста, учитывайте следующее:

- a. Позволит ли предполагаемый факт, что риск идентификации субъекта данных третьей стороной (то есть стороной, не связанной договорными обязательствами) через контактный адрес электронной почты, привязанный к регистрации, представляется незначительным, считать такие электронные адреса фактически «анонимными» для указанных третьих сторон в соответствии с критерием *Брейера*?
- b. Если нет, то как выбор контактного адреса электронной почты (с привязкой к владельцу домена или к регистрации) повлияет на результат проверки баланса законных интересов в соответствии со статьей 6(1)(f)? В какой степени использование адреса электронной почты с привязкой к регистрации уменьшит воздействие публикации на интересы или основные права и свободы субъекта данных?

Изменится ли ответ на эти вопросы, если основной целью публикации маскированного адреса электронной почты является поддержка статистических исследований и аналитики, а не общение с субъектом данных?

Анализ

66. Наш ответ начинается с ответа на подвопрос «*Позволит ли предполагаемый факт, что риск идентификации субъекта данных третьей стороной (то есть стороной, не связанной договорными обязательствами) через контактный адрес электронной почты, привязанный к регистрации, представляется незначительным, считать такие электронные адреса фактически «анонимными» для указанных третьих сторон в соответствии с критерием Брейера*», чтобы объяснить, почему мы считаем, что GDPR останется применимым в случае применения контактного адреса электронной почты, привязанного к регистрации. Затем мы перейдем к более широким аспектам вашего вопроса, касающимся соблюдения GDPR.

Анонимность

67. Мы придерживаемся мнения, выраженного в нашем меморандуме от 4 февраля 2020 года, что при любом из вариантов (контактный адрес электронной почты с привязкой к владельцу домена или с привязкой к регистрации) сохраняется высокая вероятность того, что публикация или автоматизированное раскрытие таких адресов электронной почты будет рассматриваться как обработка персональных данных.
68. Для оценки применимости GDPR к обработке электронных данных (при условии, что соблюдается критерий территориальности GDPR и не применяются положения, регулирующие только определенные конкретные обстоятельства) используется двухкомпонентная проверка:
- 68.1 Во-первых, должна осуществляться обработка информации, относящейся к конкретному физическому лицу, с которым связаны эти данные (и их обработка) «содержание, цель или последствия». Это критерий «*Новака*»⁹⁶/«относится к».
- 68.2 Во-вторых, это конкретное физическое лицо должно быть «идентифицировано или поддаваться идентификации», то есть должны существовать «средства, которые с достаточной вероятностью могут быть использованы, такие как обособление данных контролером либо другим лицом для прямой или косвенной идентификации физического лица»⁹⁷. «Идентификация» не обязательно означает установление подлинного имени человека; скорее, она имеет более общее значение, обычно связанное с возможностью конкретно «выделить» кого-то для иного обращения (выделение)⁹⁸ и/или возможностью собрать/связать больше данных о нем (умозаключение и/или связывание)⁹⁹. Технический идентификатор — даже случайно

⁹⁶ Решение Европейского суда по правам человека по делу C-434/16 *Новак*, ECLI:EU:C:2017:994, пункт 35.

⁹⁷ GDPR, преамбула 26

⁹⁸ Как цитировалось выше, в преамбуле 26 GDPR конкретно говорится о «выделении» при обсуждении средств, которые с достаточной степенью вероятности могут быть использованы для идентификации субъекта данных.

⁹⁹ Выделение, возможность привязки и умозаключение — это три составляющие критерия анонимизации, предложенные Рабочей группой 29-й статьи в ее Мнении 05/2014 о методах анонимизации (WP 216): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

сгенерированный — может быть достаточным для таких целей, особенно если он связан с другой информацией о человеке, позволяющей легко отличить его от кого-то другого¹⁰⁰. Не существует «с достаточной долей вероятности средств» восстановления идентификации, если такая деятельность «запрещена законом или практически невозможна в силу того, что требует непропорционально больших усилий с точки зрения времени, затрат и человеческих ресурсов, так что риск идентификации в действительности кажется незначительным»¹⁰¹. Это критерий «Брейера»/«возможность идентификации».

69. Наше мнение, высказанное выше, заключается в том, что обработка этих псевдонимных адресов электронной почты, скорее всего, будет рассматриваться как соответствующая обоим критериям в той степени, в которой целью обработки является предоставление средств связи с субъектами данных.

Критерий *Новака*

70. Что касается критерия *Новака*, когда контакт является физическим лицом, такие адреса будут маскироваться псевдонимами реального адреса электронной почты, используемого этим лицом. В свете этого:

70.1 Если целью/предполагаемым результатом обработки этих данных является возможность переписки с получателем (то есть, зачастую, с конкретным субъектом данных), то с учетом критерия *Новака* суда ЕС (СЖЕУ) эта «цель» и/или «результат» означает наличие связи с конкретным физическим лицом¹⁰².

70.2 Напротив, чисто статистическая обработка, направленная на создание *агрегированных* показателей (описывающих относительно большие массивы), например подсчет количества созданных псевдонимов контактных лиц, может *не* подпадать под действие GDPR. Это связано с тем, что *содержание* случайно сгенерированного контактного псевдонима не имеет связи с конкретным человеком, по крайней мере, в сценарии контакта по электронной почте, привязанной к регистрации, и — опять же, предположительно — ни *цель*, ни *результат* создания совокупных данных статистических исследований не несет в себе связи с конкретным физическим лицом; скорее, совокупная статистика описывает и выделяет *массивы/группы* (например, по стране, регистратуре, регистратору и так далее).

¹⁰⁰ По этому вопросу см. преамбулу 30 GDPR («Физические лица могут быть соотнесены с онлайн-идентификаторами, предоставляемыми их устройствами, приложениями, инструментами и протоколами, такими как IP-адреса, идентификаторы cookie или другие идентификаторы, например радиочастотные идентификационные метки. Это может оставлять следы, которые, в частности, в сочетании с уникальными идентификаторами и другой информацией, полученной серверами, могут использоваться для создания профилей физических лиц и их идентификации».)

¹⁰¹ Решение Европейского суда по правам человека по делу C-582/14 *Брейер*, ECLI:EU:C:2016:779, пункты 45 и 46.

¹⁰² В некоторых случаях контактный адрес получателя может быть коллективным почтовым ящиком (например, enquiries@example.com), и в этом случае замаскированный контактный адрес, скорее всего, не является персональными данными, независимо от применения критериев *Новака* или *Брейера*.

Критерий *Новака*, возможно, не будет выполняться в отношении этого класса обработки (но обратите внимание, что его следует отличать от сбора статистики, направленной на создание новой информации о любом конкретном субъекте данных или его классификацию — например, подсчет количества доменных имен, связанных с конкретным контактным адресом электронной почты, привязанным к владельцу домена).

70.3 Однако на практике мы не считаем возможным утверждать, что единственной целью создания и публикации контактных псевдонимов является только описанная выше обобщенная статистическая обработка. Если бы это было так, необходимость указывать адрес электронной почты полностью бы отсутствовала. Тот факт, что указан адрес электронной почты, говорит о том, что важной целью создания и публикации контактных псевдонимов всегда будет предоставление возможности связаться с конкретными лицами. Соответственно, хотя *некоторые* виды обработки (для получения совокупной статистики) могут выходить за рамки действия GDPR на основании критерия *Новака*, соблюдение GDPR, по всей видимости, будет оставаться проблемой, по крайней мере в том, что касается *других* целей обработки.

70.4 Мы также должны предостеречь от чрезмерного увлечения аргументами, основанными на критерии *Новака*. Хотя это постановление повторяет ранние рекомендации Рабочей группы 29-й статьи¹⁰³, нам не известно о систематическом использовании критерия *Новака* в анализе и рекомендациях судов и надзорных органов, применяющих GDPR. Например, по состоянию на начало апреля 2021 года поиск на сайте Бельгийского органа защиты данных на всех доступных языках выявил (i) только две прямые ссылки на дело *Новака*, и только по не относящимся к данному вопросу пунктам; и (ii) по-видимому, нет никаких ссылок на ключевую фразу «содержание, цель или результат» из критерия *Новака*. Объяснение этим органом (в его терминологии) термина «персональные данные» сосредоточено исключительно на критерии *Брейера*, то есть на возможности идентификации субъекта данных¹⁰⁴. Другие органы власти могут придерживаться иной точки зрения (например, орган власти Великобритании действительно обсуждает критерий «содержание, цель или результат» и резюмирует его влияние следующим образом: «Чтобы информация представляла собой персональные данные, она должна «относиться к» идентифицируемому физическому лицу. Это означает, что она не просто идентифицирует его, а должна каким-то образом касаться конкретного человека. (...) Данные могут ссылаться на идентифицируемое физическое лицо, но не быть при этом

¹⁰³ WP 136, стр. 10.

¹⁰⁴ <https://www.autoriteprotectiondonnees.be/citoyen/vie-privee/lexique>

персональными данными об этом лице, поскольку эта информация к нему не относится»¹⁰⁵.)

- 70.5 Более того, авторитеты в этой области не только не всегда делают существенный акцент на критерии *Новака*, но *если* они и делают это, то могут применять совершенно разные подходы к его интерпретации. Различия во мнениях могут, в частности, касаться части «содержание» критерия «содержание, цель или результат». Рабочая группа 29-й статьи в своем *Мнении 4/2007 о концепции персональных данных* (WP 136)¹⁰⁶ поясняет, что «элемент "содержание" присутствует в тех случаях, когда — в соответствии с наиболее очевидным и распространенным в обществе пониманием слова "относиться" — предоставляется информация о конкретном лице, независимо от цели контролера данных или третьей стороны, или влияния этой информации на субъект данных». Если это объяснение верно, то суд или регулирующий орган может прийти к выводу, что публикация адреса электронной почты (даже случайно сгенерированного) для контакта, связанного с регистрацией домена, *по своей сути* является публикацией информации об этом лице, потому что сообщает нам, как связаться с этим человеком. Однако это проблематичная точка зрения, поскольку она «заимствует» рассуждения из критериев *цель и результат* (рассматривает возможную цель информации, а не содержание самой информации) и основывается на *гипотетической* цели/результате, а не на *фактической* цели/результате обработки — таким образом, полностью упуская две трети критерия «содержание, цель или результат». Как с точки зрения логики, так и с точки зрения верховенства закона (ясность/определенность), это проблематично. С более простой точки зрения, нечто случайно сгенерированное (as876bnk@example.com) является чистым выражением случайного «шума» — мгновенного снимка электрического состояния схемы «генератора случайных чисел» компьютера. Таким образом, оно не содержит и не может само по себе «содержать» какую-либо информацию о каком-либо человеке. Если бы оно само по себе *передавало* информацию о человеке, то, по логике вещей, не было бы случайным. С этой точки зрения, случайно сгенерированный адрес не проходит проверку по критерию «содержание»; вместо этого необходимо сосредоточиться на цели и/или результате обработки данных.
- 70.6 Таким образом, очевидно, что существует значительный риск разногласий, по крайней мере, с некоторыми органами власти, если аргументы опираются на дело *Новака*.

¹⁰⁵ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/#pd5>

¹⁰⁶ Рабочая группа 29-й статьи, *Мнение 4/2007 о концепции персональных данных* (WP 136), стр. 10. Доступно в интернете: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Критерий *Брейера*

71. Что касается критерия *Брейера*, в этом деле CJEU провел мысленный эксперимент: если произошла кибератака, контролер, владеющий IP-адресом (и, как мы предполагаем — хотя суд не уточняет этот момент — временной меткой, указывающей, когда этот IP-адрес использовался интересующим нас устройством/лицом), может передать эту информацию в полицию/судебные органы. CJEU решил, что в этом случае органы власти часто будут иметь полномочия затребовать соответствующую информацию у интернет-провайдера, который присвоил этот IP-адрес, и, следовательно, возбудить судебное преследование (хотя CJEU попросил национальные суды проверить это предположение). Таким образом, CJEU постановил, что, если такой сценарий не запрещен законом или практически невозможен, существуют «с достаточной долей вероятности средства» идентификации субъекта данных.
72. Ключевым моментом здесь является то, что, хотя третья сторона может просто узнать контактный адрес электронной почты, привязанный к владельцу домена или регистрации, компетентные органы власти могут соотнести его с закрытыми регистрационными данными, хранящимися у сторон, связанных договорными обязательствами, что позволит вновь идентифицировать личность. Насколько нам известно, это не всегда требует «практически невозможных» усилий и не всегда запрещено законом.
73. То есть даже в том, что касается *третьих лиц*, распространение и использование таких контактных псевдонимов может рассматриваться как обработка персональных данных.
74. Что касается *сторон, связанной договорными обязательствами*, которая знает, какой контактный псевдоним она присвоила владельцу домена/назначенному владельцем домена контактному лицу, создание и размещение таких адресов, а также предоставление их для использования другими лицами, почти наверняка является обработкой персональных данных (когда контактные лица являются физическими лицами).

Риск соответствующих представленных вариантов

75. Разъяснив наше мнение о том, что для любого из вариантов GDPR сохраняет свою актуальность, мы переходим к вашей просьбе сравнить риски, связанные с (а) публикацией в интернете или (b) автоматическим раскрытием (i) контактного адреса электронной почты с привязкой к владельцу домена, с одной стороны, и (ii) контактного адреса электронной почты с привязкой к регистрации, с другой стороны.

76. Наше резюме (в котором отражены важные предположения и оговорки, приведенные далее в этом ответе) следующее:

		Контактный адрес электронной почты с привязкой к владельцу домена	Контактный адрес электронной почты с привязкой к регистрации
Публикация в интернете	в	Средний	Низкий
Автоматизированное раскрытие		Низкий	Минимальный

77. Исходя из применения принципов GDPR, распространение (путем публикации в интернете или автоматического раскрытия) псевдонимов электронной почты, привязанных к регистрации, влечет меньший риск по сравнению с псевдонимами электронной почты, привязанными к владельцу домена.
78. Причина в том, что кто-то, владеющий адресом электронной почты с привязкой к владельцу домена, может узнать больше информации о субъекте данных, в частности, о том, с какими еще доменными именами связан этот субъект данных. Это связано с тем, что если для субъекта данных не будет указан другой *реальный* контактный адрес для каждого зарегистрированного им домена, то при каждой регистрации будет использоваться один и тот же псевдоним электронной почты.
79. Публикация таких сведений в интернете может облегчить создание таких профилей и, возможно, даже создание инструмента обратного поиска («для данного контактного адреса электронной почты, привязанного к регистрации, с какими доменными именами связан этот контакт?»).
80. Автоматическое раскрытие информации, само по себе, предположительно, усложнит эту задачу, поскольку, если в составе инструментов автоматического раскрытия информации не предлагается *намеренно* функция обратного поиска¹⁰⁷, заявителям, предположительно, придется запрашивать потенциально большое количество доменных имен для сбора достаточной информации, чтобы иметь возможность выполнить сопоставление и начать создание (неполной) функции обратного поиска. Однако отправители запросов, у которых есть заранее составленный список конкретных доменных имен (например, предполагаемые «зеркала» сайта, на котором размещен незаконный контент), могут определить, был ли предоставлен один и тот же адрес электронной почты для некоторых или

¹⁰⁷ Такие функции перед внедрением требуют тщательного рассмотрения. Старые указания по данному вопросу см. в Мнении 5/2000 Рабочей группы 29-й статьи «Использование общедоступных каталогов для услуг обратного или многокритериального поиска (обратные каталоги)» (WP 33): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf

всех этих сайтов. Таким образом, даже в сценарии автоматического раскрытия информации, использование схемы, где применяется контактный адрес электронной почты, привязанный к владельцу домена, сопряжено с дополнительными рисками для конфиденциальности, по сравнению со схемой, в которой применяется контактный адрес электронной почты, привязанный к регистрации.

81. Соответственно, принимая во внимание следующие соображения:

81.1 Необходимость соблюдения правила минимизации данных GDPR;

81.2 Необходимость соблюдения принципа «конфиденциальности по замыслу и по умолчанию»;

81.3 Что опора на статью 6(1)(f) GDPR (правовая основа «законные интересы») является более надежной, когда проектирование системы минимизирует ущерб «интересам или основным правам и свободам субъекта данных, которые требуют защиты персональных данных»; и

81.4 При оценке того, следует ли налагать штрафы на контролера и в каком размере, органы власти должны учитывать, *помимо прочего*, «тяжесть» нарушения, «объем» обработки, «уровень ущерба, понесенного субъектами данных», «любые действия, предпринятые контролером или обработчиком для смягчения ущерба, понесенного субъектами данных», и «степень ответственности контролера или обработчика, принимаемая во внимание технические и организационные меры, принятые ими в соответствии со статьями 25 и 32» (см. GDPR, статья 83),

мы считаем, что схема на основе контактного адреса электронной почты с привязкой к регистрации влечет меньший риск, чем схема на основе контактного адреса электронной почты с привязкой к владельцу домена.

82. Разъяснив баланс рисков по оси «схема с привязкой регистрации в сравнении со схемой с привязкой к владельцу домена», мы переходим к составлению рисков публикации в интернете и автоматического раскрытия информации.

83. Риск, характерный для схем как с привязкой регистрации, так и с привязкой к владельцу домена, заключается в спаме или других нежелательных электронных письмах; такая «адресуемость», надо полагать, является одним из аспектов конфиденциальности¹⁰⁸. Спам является давней проблемой систем WHOIS; он был предметом исследования Консультативного комитета по безопасности и стабильности ICANN в 2007 году, который пришел к выводу, что «отображение адресов электронной почты в ответ на запросы

¹⁰⁸ Преамбула 40 Директивы 2002/58/ЕС («Директива о конфиденциальности и электронных сообщениях» ЕС) гласит: «Следует предусмотреть средства защиты абонентов от вторжения в их частную жизнь путем отправки нежелательных сообщений в целях прямого маркетинга, в частности, с помощью автоматических телефонных аппаратов, телефаксов и электронной почты, включая SMS-сообщения».

- WHOIS действительно способствует получению спама, хотя и является всего лишь одной из множества причин»¹⁰⁹.
84. Соответственно, независимо от того, используется ли контактный адрес электронной почты с привязкой к владельцу домена или к регистрации, должны быть приняты эффективные меры для решения проблемы доступности адресов для спамеров (например, использование технических средств для предотвращения «сбора» таких адресов; и/или фильтрация нежелательных сообщений до их доставки адресату).
85. По сравнению с публикацией в интернете, мы предполагаем, что автоматизированное раскрытие информации позволяет расширить возможности оценки мотивов и источников запросов, а также мониторинга/аудита и применения мер защиты в отношении таких запросов (например, ограничение частоты), то есть позволяет расширить возможности принятия таких мер, которые позволят снизить ответственность с учетом факторов, изложенных в пункте 81 выше. Поэтому автоматическое раскрытие информации, видимо, по своей природе влечет меньший риск по сравнению с публикацией в интернете.
86. Эти потенциальные преимущества автоматизированного раскрытия информации по сравнению с публикацией в интернете также могут представлять собой преимущества с точки зрения статьи 25 GDPR (конфиденциальность по замыслу и по умолчанию). В частности, необходимо подумать о том, чтобы процедура публикации в интернете соответствовала статье 25(2) GDPR, «такие меры должны гарантировать, что по умолчанию персональные данные не будут доступны без вмешательства физического лица неопределенному числу физических лиц»¹¹⁰.
87. Тем не менее, если будут приняты эффективные меры по борьбе со спамом, а также если будет использован подход с привязкой к регистрации (в силу его преимуществ, о которых говорилось ранее), то, учитывая низкую полезность данных, трудно представить, каким образом их публикация в интернете повлечет за собой значительный риск для конфиденциальности или безопасности данных.

* * *

¹⁰⁹ SAC 023: Является ли служба WHOIS источником адресов электронной почты для спамеров?,

Основные положения. Доступно в интернете: <https://www.icann.org/en/system/files/files/sac-023-en.pdf>

¹¹⁰ В пункте 56 своих Указаний 4/2019 по статье 25 «Защита данных по замыслу и по умолчанию»,

ред. 2.0 EDPB разъясняет, что «контролер должен по умолчанию ограничить доступность и предоставить субъекту данных возможность вмешаться, прежде чем опубликовать или иным образом сделать доступными персональные данные о субъекте данных неопределенному числу физических лиц».

Доступно в интернете: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf