# Структурное описание принципа подотчетности в GDPR на основе ICO Accountability Framework

v.1.0 2022.01.10 © Алексей Мунтян | Alexey Muntyan
muntyan.alexey@gmail.com

Согласно ст.5(2) GDPR контролёр несет ответственность за соблюдение принципов обработки ПД, зафиксированных в ст.5(1) GDPR, и должен быть в состоянии продемонстрировать его соблюдение («Принцип подотчетности»). В п.82 Преамбулы GDPR указано, что для демонстрации соответствия GDPR контролёр или процессор должен вести учет деятельности по обработке, за которую он отвечает. Каждый контролёр и процессор обязан сотрудничать с надзорным органом и по запросу предоставлять в его распоряжение указанные учетные сведения в целях мониторинга процесса обработки.

Одним из наиболее проработанных и признаваемых в экспертной среде инструментом по созданию и поддержанию комплексной программы управления защитой ПД (Comprehensive Privacy Management Programme), а также по соблюдению принципа подотчётности, является Accountability Framework[1], разработанный Офисом Уполномоченного по информации в Соединенном Королевстве (Information Commissioner's Office). На основе структуры и содержания указанного документа ниже описано **78 контролей (включающих в себя около 360 элементов) подотчетности, сгруппированных в 10 категорий**, где каждый из контролей направлен на обеспечение организацией возможности демонстрации соблюдения требований GDPR.

Данное описание не является дословным переводом на русский язык Accountability Framework, включает в себя несколько дополнительных контролей, а также содержит нормативные ссылки. Отдельным перечнем приведена документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR.

**Навигация:**



*Описание контролей демонстрации соблюдения требований GDPR*

## 1. Руководство и надзор

Основополагающим элементом является эффективное руководство и надзор. Это включает в себя обеспечение четкой ответственности персонала[2] за деятельность, связанную с обработкой и защитой данных, на стратегическом и функциональном уровне. В некоторых организациях по закону требуется должность DPO, но каждая организация должна выделять достаточно ресурсов и следить за тем, чтобы защита данных была общей ответственностью, а не задачей отдельного человека, непосредственно выполняющего функции по защите данных. Руководство организации должно нести свою долю ответственности за защиту данных, и оно должно подавать пример организованного, активного и конструктивного подхода к защите данных, который лежит в основе всего остального.

| | | |
|---|---|---|
| 1.1 | *Контроль* | **Организационная структура** |
| | *Описание* | Существует организационная структура для управления и практической реализации защиты данных, которая обеспечивает эффективное руководство и надзор, четкий порядок и обязанности, а также эффективные коммуникации. |
| | *Ожидания* | • Руководство организации несет общую ответственность за управление и практическую реализацию защиты данных.<br>• Лица, принимающие решения, подают пример и поощряют активную, конструктивную культуру соблюдения требований по защите данных.<br>• Существует четкий порядок коммуникаций между соответствующими группами.<br>• Политики и процедуры четко определяют организационную структуру управления и практической реализации защиты данных.<br>• В должностных инструкциях четко прописаны обязанности и порядок предоставления отчетности руководству.<br>• Должностные инструкции являются актуальными, соответствуют поставленной цели и регулярно пересматриваются.<br>• Персонал, обеспечивающий защиту данных, понимает организационную структуру и свои обязанности. |
| | *Ссылки* | • GDPR: ст.24; rc.74<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 1.2 | *Контроль* | **Назначение DPO** |

[1] См. https://ico.org.uk/for-organisations/accountability-framework/

[2] Под «персоналом» понимается совокупность всех сотрудников организации, а также иных физических лиц, осуществляющих производственные, управленческие или иные функции в интересах организации на основании трудового договора или договора гражданско-правового характера.

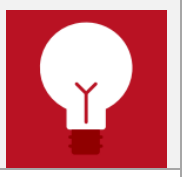
| | | |
|---|---|---|
| | *Описание* | Если необходимо назначить DPO в соответствии требованиями законодательства, организация гарантирует, что функция DPO должным образом поддерживается и охватывает все соответствующие требования и обязанности. |
| | *Ожидания* | • DPO отвечает за соблюдение требований по защите данных, политики и процедуры по защите данных, повышение осведомленности, обучение и аудит.<br>• DPO обладает профессиональными знаниями в области законодательства и практики защиты данных.<br>• У DPO есть полномочия, поддержка руководства и ресурсы для эффективного выполнения работы.<br>• Организация надлежащим образом уведомила соответствующий SA о назначении DPO.<br>• Если организация не обязана назначать DPO и не назначает такое лицо, то это решение надлежащим образом документировано.<br>• Если организация не назначает DPO, то ответственность за соблюдение требований по защите данных надлежащим образом распределяется внутри организации, и у организации достаточно персонала и ресурсов для выполнения требований законодательства о защите данных. |
| | *Ссылки* | • GDPR: ст.37, 39; rc.97<br>• Guidelines on Data Protection Officers ('DPO'), WP243 rev.01<br>• Guidelines pratique RGPD - Délégués à la protection des données (Commission Nationale de l'Informatique et des Libertés, Novembre 2021)<br>• Guidance on Appropriate Qualifications for DPOs (Data Protection Commission, July 2019) |
| 1.3 | *Контроль* | **Подотчетность DPO** |
| | *Описание* | DPO независим и беспристрастен. Он должен отчитываться перед руководством организации, и персонал должен четко представлять, как с ним связаться. |
| | *Ожидания* | • Персонал знает, кто такой DPO, какова его функция и как с ним связаться.<br>• Все вопросы, связанные с защитой данных, своевременно доводятся до сведения DPO.<br>• Организация следует рекомендациям DPO и учитывает его экспертизу по защите данных.<br>• DPO выполняет свои задачи независимо, без каких-либо конфликтов интересов, и не принимает прямых оперативных решений относительно способа и целей обработки ПД в организации.<br>• DPO напрямую консультирует руководство организации, принимающее решения, и поднимает вопросы на самом высоком уровне управления.<br>• DPO регулярно информирует руководство организации об актуальных вопросах соблюдения требований по защите данных в организации. |
| | *Ссылки* | • GDPR: ст.38; rc.97<br>• Guidelines on Data Protection Officers ('DPO'), WP243 rev.01<br>• Guidelines pratique RGPD - Délégués à la protection des données (Commission Nationale de l'Informatique et des Libertés, Novembre 2021)<br>• Guidance on Appropriate Qualifications for DPOs (Data Protection Commission, July 2019) |
| 1.4 | *Контроль* | **Оперативные функции** |
| | *Описание* | Оперативные функции организации поддерживают управление и практическую реализацию защиты данных. |
| | *Ожидания* | • Персонал, обеспечивающий защиту данных, несёт четкую ответственность за обеспечение соответствия организации требованиям по защите данных.<br>• Персонал эффективно управляет всеми записями и обеспечивают их безопасность.<br>• Персонал, обеспечивающий защиту данных, помогает внедрять и поддерживать политики и процедуры защиты данных на локальном уровне.<br>• Персонал, обеспечивающий защиту данных, обладает полномочиями, поддержкой и ресурсами для эффективного выполнения своих обязанностей. |
| | *Ссылки* | • GDPR: ст.24; rc.74<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 1.5 | *Контроль* | **Группа надзора** |
| | *Описание* | Группа надзора обеспечивает для организации руководство и управление основными аспектами защиты данных. |
| | *Ожидания* | • Ключевой персонал, например генеральный директор, регулярно посещает собрания группы надзора.<br>• Группу возглавляет соответствующе уполномоченное лицо, например, DPO или старший ответственный за управление информационными рисками (SIRO).<br>• Цели группы определены через четкую постановку задач.<br>• Содержание и результаты собраний группы фиксируются (протоколируются).<br>• Группа охватывает полный спектр тем, связанных с защитой данных, включая KPI, проблемы и риски.<br>• У группы есть план работы или действий, выполнение которого регулярно отслеживается.<br>• Руководство организации рассматривает вопросы управления и практической реализацию защиты данных, а также риски, о которых руководству сообщает группа надзора. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 1.6 | *Контроль* | **Собрания оперативных групп** |
| | *Описание* | В организации группы оперативного уровня проводят собрания для обсуждения и координации деятельности по управлению и практической реализаций защиты данных. |
| | *Ожидания* | • Группы регулярно проводят собрания, в которых принимает участие соответствующий персонал.<br>• Группы составляют протоколы собраний и планы действий.<br>• Повестка собраний демонстрирует, что группы регулярно обсуждают соответствующие вопросы управления и практической реализацию защиты данных.<br>• О любых возникающих проблемах и рисках в области управления и практической реализацию защиты данных сообщается группе надзора. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| **2. Политики и процедуры** | | |

Политики и процедуры обеспечивают ясность и последовательность, информируя персонал о том, что нужно делать и почему. Политики также могут описывать цели, ценности и положительный настрой. GDPR требует внедрения политики защиты данных там, где это необходимо. Область применения политики и ее уровень детализации варьируется, но эффективные политики и процедуры защиты данных могут помочь организации предпринять практические шаги для выполнения юридических обязательств.

| | | |
|---|---|---|
| 2.1 | *Контроль* | **Указания и поддержка** |
| | *Описание* | Политики и процедуры организации предоставляют персоналу достаточные указания для понимания его функций и обязанностей в отношении управления и практической реализации защиты данных. |
| | *Ожидания* | • Основы политики защиты данных вытекают из стратегического бизнес-планирования в области управления и практической реализации защиты данных, одобренного руководством организации.<br>• Политика охватывает защиту данных, управление записями и ИБ.<br>• Организация обеспечивает доступность операционных процедур, руководств и рекомендаций для поддержки политики защиты данных и обеспечивает оперативное руководство персоналом, ответственным за защиту данных.<br>• Политики и процедуры четко определяют функции и обязанности персонала. |
| | *Ссылки* | • GDPR: ст.24<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 2.2 | *Контроль* | **Рассмотрение и утверждение** |
| | *Описание* | В организации существует надлежащий процесс рассмотрения и утверждения внутренних документов для гарантии того, что политики и процедуры являются последовательными и эффективными. |
| | *Ожидания* | • Все политики и процедуры соответствуют согласованному формату и стилю.<br>• Соответствующий уполномоченный сотрудник рассматривает/пересматривает и утверждает все новые и существующие политики и процедуры.<br>• Существующие политики и процедуры пересматриваются в соответствии с задокументированными датами пересмотра, поддерживаются актуальными и соответствуют поставленным целям.<br>• Политики и процедуры обновляются без неоправданных задержек, когда они требуют изменений, например, из-за операционных перемен, судебных или регуляторных решений или изменений в лучших практиках.<br>• Политика, процедуры и руководства содержат информацию об управлении документами, включая номер версии, владельца, дату пересмотра и историю изменений. |
| | *Ссылки* | • Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 2.3 | *Контроль* | **Осведомленность персонала** |
| | *Описание* | Персонал полностью осведомлен о политиках и процедурах управления и практической реализации защиты данных, которые имеют отношение к его функциям. |
| | *Ожидания* | • Персонал ознакомлен и понимает политики и процедуры, в том числе, почему важно их внедрять и соблюдать.<br>• Персонал своевременно информируется об обновлении политик и процедур.<br>• Политики и процедуры доступны для всего персонала на сайте организации во внутренней сети (или в аналогичном общем доступе) или предоставляется персоналу в других форматах.<br>• Руководства, плакаты или публикации помогают подчеркнуть ключевые идеи и повысить осведомленность персонала о политиках и процедурах. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 2.4 | *Контроль* | **DPDD** |
| | *Описание* | Политики и процедуры способствуют применению подхода DPDD во всей организации. |
| | *Ожидания* | • При необходимости, внутренние документы организации рассматриваются и оцениваются с учетом требований защиты данных.<br>• Политики и процедуры обеспечивают внимание к вопросам защиты данных при разработке и внедрении систем, услуг, продуктов и деловой практики, связанных с ПД, и чтобы обеспечение защиты ПД по умолчанию.<br>• Подход организации к реализации принципов защиты данных и защите прав физических лиц, таких как минимизация данных, псевдонимизация и ограничение целей, изложен в политиках и процедурах.<br>• ПД уязвимых групп, например, детей, получают дополнительную защиту в рамках политик и процедур. |
| | *Ссылки* | • GDPR: ст.25; rc.78<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPB Guidelines 3/2019 on Processing of Personal Data through Video Devices<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Opinion 2/2017 on data processing at work - WP249<br>• A Guidelines to Privacy by Design (Agencia Española de Protección de Datos, October 2019)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020) |

### 3. Обучение и осведомленность

Это гарантирует, что весь персонал пройдет соответствующее обучение программе обеспечения защиты данных, включая ее цели, ее требования к персоналу и какие обязанности персонал несёт. Обучение должно быть актуальным, точным и своевременным. Обучение и осведомленность являются ключом к практическому применению политик, процедур и руководств.



| | | |
|---|---|---|
| 3.1 | *Контроль* | **Программы обучения персонала** |
| | *Описание* | Существует учебная программа по управлению и практической реализации защиты данных для всего персонала. |
| | *Ожидания* | • Программа учитывает национальные и отраслевые требования.<br>• Программа является всеобъемлющей и включает обучение всего персонала ключевым областям защиты данных, таким как обработка запросов, обмен данными, ИБ, нарушение безопасности ПД и управление записями.<br>• Учитываются потребности в обучении всего персонала, и эта информация используется для составления программы обучения. |

| | | |
|---|---|---|
| | | • Обязанности по организации обучения в организации распределены между соответствующими лицами, и есть планы или стратегии обучения для удовлетворения потребностей в обучении в согласованные сроки.<br>• Есть в наличии специальные и обученные лица для проведения обучения всех сотрудников.<br>• Программа регулярно пересматривается для подтверждения ее точности и актуальности.<br>• Руководство организации одобрило (утвердило) программу. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 3.2 | *Контроль* | **Вводное и повторное обучение** |
| | *Описание* | Программа обучения включает вводное и повторное обучение для всего персонала по вопросам управления и практической реализации защиты данных. |
| | *Ожидания* | • Соответствующий сотрудник, например, DPO или менеджер по управлению информацией, контролирует или утверждает вводный курс обучения.<br>• Персонал проходят вводное и повторное обучение, независимо от того, как долго они будут работать в организации, их типа контракта или класса.<br>• Персонал проходят вводное обучение до получения доступа к ПД и в течение одного месяца с даты начала их работы.<br>• Персонал проходит повторное обучение через соответствующие промежутки времени. |
| | *Ссылки* | • GDPR: ст.39<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 3.3 | *Контроль* | **Ключевой персонал** |
| | *Описание* | Персонал с ключевыми обязанностями по защите данных (например, DPO, группы управления записями) проходят дополнительное обучение и повышение квалификации сверх базового уровня, предоставляемого всему персоналу. |
| | *Ожидания* | • Проводится анализ потребностей в обучении ключевого персонала управлению и практической реализации защиты данных, чтобы составить план обучения и обеспечить его соответствие обязанностям конкретного сотрудника.<br>• Требования к обучению и навыкам подробно описаны в должностных обязанностях ключевого персонала.<br>• Есть доказательства прохождения ключевым персоналом актуального и соответствующего специализированного обучения и повышения квалификации, а также прохождения соответствующего повторного обучения. |
| | *Ссылки* | • GDPR: ст.39<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 3.4 | *Контроль* | **Контроль результатов обучения** |
| | *Описание* | Организация может продемонстрировать, что персонал понимает суть обучения, и проверяет его понимание и соответствующим образом контролируете его, например, с помощью оценок или опросов. |
| | *Ожидания* | • Проводится оценка в конце обучения, чтобы проверить понимание персонала и убедиться, что обучение эффективно, для чего можно установить минимальный проходной балл.<br>• Сохраняются копии предоставленных учебных материалов, а также подробная информация о том, кто и когда проходил обучение.<br>• Прохождение обучения контролируется в соответствии с организационными требованиями на всех уровнях организации и ведется учет персонал, который еще не прошёл обучение.<br>• Персонал может оставлять отзывы о получаемом им обучении. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 3.5 | *Контроль* | **Повышение осведомленности** |
| | *Описание* | Регулярно повышается осведомленность персонала об управлении и практической реализации защиты данных, а также о связанных с этим политиках и процедурах на собраниях или мероприятиях для персонала. Персоналу обеспечен удобный доступ к соответствующим материалам. |
| | *Ожидания* | • Наличие доказательства того, что организация регулярно использует различные подходящие методы для повышения осведомленности персонала и повышения значимости управления и практической реализации защиты данных, например, с помощью электронных писем, групповых брифингов и собраний, плакатов, раздаточных материалов и блогов.<br>• Персоналу обеспечен удобный доступ к соответствующим материалам и предоставлена возможность узнать, к кому обращаться в случае возникновения вопросов, связанных с управлением и практической реализацией защиты данных. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |

### 4. Права субъектов данных

GDPR направлен на расширение прав и возможностей субъектов данных и предоставление им большего контроля над своими ПД посредством ряда правомочий, которые организация должна эффективно поддерживать. Соблюдение прав субъектов данных сводит к минимуму риски как для субъектов данных, так и для организации. Это поможет организации соблюдать другие требования по защите данных, такие как принципы обработки ПД. Соблюдение требований по защите данных укрепляет репутацию организации и дает ей конкурентное преимущество, поскольку повышает доверие и уверенность субъектов данных в том, что организация обращается с ПД надлежащим образом.

| | | |
|---|---|---|
| 4.1 | *Контроль* | **Информирование субъектов данных и выявление запросов** |
| | *Описание* | Организация информирует субъектов данных об их правах, и весь персонал знает, как выявлять и обрабатывать как устные, так и письменные запросы. |
| | *Ожидания* | • Субъектам данных предоставляется четкая и актуальная информация об их правах и о том, как ими воспользоваться.<br>• В политиках и процедурах изложен порядок рассмотрения запросов субъектов данных об их правах.<br>• Весь персонал проходит обучение и получает рекомендации о том, как выявить запрос и куда его отправить. |
| | *Ссылки* | • GDPR: ст.11-23; rc.57-73<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• EDPB Statement on Restrictions on Data Subject Rights in Connection to the State of Emergency in Member States |

| | | |
|---|---|---|
| | | • EDPB Guidelines 10/2020 on Restrictions under Article 23 GDPR<br>• Guidelines on the Right of access (Information Commissioner's Office, October 2020) |
| 4.2 | *Контроль* | **Ресурсы** |
| | *Описание* | У организации есть в наличии соответствующие ресурсы для обработки запросов субъектов данных об их данных. |
| | *Ожидания* | • Конкретное лицо(а) или подразделение отвечают за управление запросами и реагирование на них.<br>• Персонал проходит специальное обучение для обработки запросов, включая регулярное повторное обучение. У организации достаточно ресурсов для обработки запросов.<br>• Если уполномоченное лицо временно отсутствует, исполняющие его обязанности лица проходят обучение по выполнению соответствующих задач.<br>• Организация может эффективно справиться с любым увеличением запросов или сокращением численности обрабатывающего их персонала. |
| | *Ссылки* | • GDPR: ст.12; rc.58 |
| 4.3 | *Контроль* | **Регистрация и отслеживание запросов** |
| | *Описание* | Организация регистрирует получение всех устных и письменных запросов от субъектов данных и ведет учетный журнал, чтобы отслеживать обработку каждого запроса. |
| | *Ожидания* | • Существуют процессы, обеспечивающие точность и обновление журнала по мере необходимости.<br>• В журнале отображаются сроки выполнения запросов, фактическая дата окончательного ответа и принятые меры.<br>• В контрольном списке записаны ключевые этапы процесса обработки запросов, например, в каких системах или подразделениях был проведен поиск. Это либо часть журнала, либо отдельный документ.<br>• Существуют записи ответов на запросы в адрес организации, а также любая раскрытая или скрытая информация из запросов на доступ к личным делам. |
| | *Ссылки* | • GDPR: ст.12; rc.59, 64<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 4.4 | *Контроль* | **Своевременные ответы** |
| | *Описание* | Организация своевременно обрабатывает запросы субъектов данных в соответствии с индивидуальными ожиданиями и установленными законом сроками. |
| | *Ожидания* | • Организация рассматривает все запросы в установленные законом сроки.<br>• Сотрудники, ответственные за обработку запросов, регулярно встречаются для обсуждения любых вопросов и проведения расследований, определения приоритетов или рассмотрения отложенных дел.<br>• Если организации требуется больше времени на ответ, она информирует субъектов данных о ходе выполнения их запроса и держите их в курсе.<br>• Если запрос отклоняется, у организации есть записи о причинах отказа, и она информирует субъектов данных о причинах любых отказов или исключений. |
| | *Ссылки* | • GDPR: ст.12; rc.59<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01 |
| 4.5 | *Контроль* | **Мониторинг и оценка эффективности** |
| | *Описание* | Организация отслеживает, как персонал обрабатывают запросы, и использует эту информацию для внесения улучшений. |
| | *Ожидания* | • Сотрудники, ответственные за обработку запросов, регулярно встречаются для обсуждения любых вопросов.<br>• Регулярно составляются отчеты об эффективности и проводится оценку качества рассмотрения дел, чтобы гарантировать, что запросы обрабатываются надлежащим образом.<br>• Отчеты регулярно предоставляются руководству организации, и оно рассматривает их и принимает решения на соответствующих собраниях.<br>• Организация анализирует любые тенденции в характере или причинах запросов для повышения эффективности или сокращения объемов. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 4.6 | *Контроль* | **Неточные или неполные данные** |
| | *Описание* | В организации имеются соответствующие системы и процедуры для изменения неточных данных, добавления дополнительных данных в неполные записи или добавления дополнительных записей при такой необходимости, в т.ч. при получении запроса субъекта. |
| | *Ожидания* | • Организация предпринимает адекватные и разумные шаги для проверки точности хранящихся ПД и, в случае необходимости, способна их исправить.<br>• Если организация уверена в том, что данные являются точными, у неё есть процедура, позволяющая объяснить это субъекту данных. Организация должна проинформировать субъекта данных о его праве подать жалобу и в соответствии с надлежащей практикой зафиксировать в системе тот факт, что физическое лицо оспаривает точность информации.<br>• Если ПД были раскрыты другим лицам, организация связывается с каждым получателем, чтобы сообщить ему об изменении, если это возможно или не требует несоразмерных усилий.<br>• В случае запроса организация сообщает субъекту данных, какие третьи лица получили ПД. |
| | *Ссылки* | • GDPR: ст.15-16, 19; rc.63-65 |
| 4.7 | *Контроль* | **Удаление данных** |
| | *Описание* | В организации существуют соответствующие методы и процедуры для удаления, ограничения или иного прекращения обработки данных при такой необходимости, в т.ч. при получении запроса субъекта. |
| | *Ожидания* | • При необходимости организация удаляет ПД из резервных систем, а также из работающих систем, и четко сообщает физическому лицу, что произойдет с его данными.<br>• Если ПД раскрываются другим лицам, организация связывается с каждым получателем, чтобы сообщить ему об удалении, если это возможно или не требует несоразмерных усилий.<br>• В случае запроса организация сообщает субъекту данных, какие третьи лица получили ПД. Если ПД были обнародованы в онлайн-среде, организация предпринимает разумные шаги, чтобы сообщить другим контролирующим лицам, если они их обрабатывают, о необходимости стереть ссылки на эти данные, их копии или воспроизведение.<br>• Организация придает особое значение запросу на удаление, если обработка осуществляется или была основана на согласии ребенка, особенно при обработке любых ПД в Интернете. |
| | *Ссылки* | • GDPR: ст.17, 19; rc.65-66 |

| | | |
|---|---|---|
| | | • EDPB Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR<br>• Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González C-131/12, WP225 |
| 4.8 | *Контроль* | **Ограничение обработки данных** |
| | *Описание* | В организации имеются соответствующие методы и процедуры для ограничения обработки ПД при такой необходимости, в т.ч. при получении запроса субъекта. |
| | *Ожидания* | • Организация ограничивает обработку ПД методом, соответствующим типу и способу обработки, например, временно переносит данные в другую систему или удаляет их с веб-сайта.<br>• Если ПД были раскрыты другим лицам, организация связывается с каждым получателем, чтобы сообщить ему об ограничении, если это возможно или не требует несоразмерных усилий.<br>• В случае запроса организация сообщает субъекту данных, какие третьи лица получили его ПД. |
| | *Ссылки* | • GDPR: ст.18-19; rc.67 |
| 4.9 | *Контроль* | **Переносимость данных** |
| | *Описание* | Субъекты данных могут безопасно перемещать, копировать или передавать свои ПД из организации в другую, не влияя при этом на данные. |
| | *Ожидания* | • По запросу субъекта данных организация предоставляет ПД в структурированном, общепринятом и машиночитаемом формате.<br>• При возможности и по запросу субъекта данных, организация может напрямую передать информацию другой организации. |
| | *Ссылки* | • GDPR: ст.20; rc.68<br>• Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01<br>• Guidelines on the Right of access (Information Commissioner's Office, October 2020) |
| 4.10 | *Контроль* | **Автоматизированное принятие решений и профилирование** |
| | *Описание* | Организация может защитить индивидуальные права субъектов данных, связанные с автоматизированным принятием решений и профилированием, особенно если обработка ПД является исключительно автоматизированной и имеет юридические или аналогичные существенные последствия для субъекта. |
| | *Ожидания* | • Выполняются дополнительные проверки для уязвимых групп субъектов, таких как дети, до внедрения автоматизированного принятия решений и профилирования.<br>• Организация собирает только необходимый минимум данных и имеет четкую политику хранения созданных профилей.<br>• Если организация использует исключительно автоматизированные решения, которые оказывают юридическое или аналогичное существенное влияние на субъектов данных, у неё есть зарегистрированный процесс, гарантирующий, что эти решения принимаются только в соответствии со ст.22 GDPR. Если это применимо, организация также должна провести DPIA.<br>• В тех случаях, когда принятие решений полностью автоматизировано и оказывает юридическое или аналогичное существенное влияние на субъектов данных, формализованная процедура позволяет субъектам данных простыми способами запрашивать вмешательство человека в процесс принятия решений, выражать свое мнение и оспаривать принятое автоматизированным способом решение.<br>• Организация проводит регулярные проверки точности и возможные недочеты в процессе автоматизированного принятия решений, чтобы убедиться, что системы работают должным образом, и использует полученные в ходе проверок данные в процессе проектирования новых процессов автоматизированного принятия решений. |
| | *Ссылки* | • GDPR: ст.22; rc.71-72<br>• EDPB Guidelines 08/2020 on the targeting of social media users<br>• EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on use of cookies (Agencia Española de Protección de Datos, January 2021)<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Guidance on Cookies and Similar Technologies (Data Protection Commission, April 2020) |
| 4.11 | *Контроль* | **Жалобы и возражения** |
| | *Описание* | В организации существуют процедуры для получения и реагирования на жалобы и возражения субъектов данных, а сами субъекты информируются об их праве на подачу жалобы или возражения. |
| | *Ожидания* | • В организации есть процедуры для рассмотрения жалоб субъектов по поводу защиты их данных и возражений субъектов против обработки их данных, а руководство организации своевременно информируется о разрешении жалоб и возражений.<br>• Контактные данные DPO или альтернативные контактные пункты находятся в открытом доступе, если субъекты данных хотят подать жалобу или заявить возражение.<br>• Организация информирует субъектов данных об их праве подать жалобу в SA в своих уведомлениях или иных документах/сведениях, направляемых субъектам данных. |
| | *Ссылки* | • GDPR: ст.13, 21; rc.69-70<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01 |

## 5. Прозрачность

Прозрачность является ключевым принципом защиты данных, который является основополагающим для подхода DPDD. Она облегчает реализацию прав субъектов данных и дает субъектам больший контроль над обработкой данных. Это особенно важно, если обработка является сложной или если она связана с детьми. Уважение частной жизни людей может дать организации конкурентное преимущество за счет повышения доверия общественности, надзорных органов и бизнес-партнеров. Открытость и честность в отношении того, что организация делает с ПД, будет способствовать заключению соглашений и обмену данными с третьими сторонами.

| | | |
|---|---|---|
| 5.1 | *Контроль* | **Содержание уведомления о защите данных** |
| | *Описание* | Информация или уведомление о защите данных (Privacy Notice) организации включает всю необходимую информацию в соответствии со ст.13-14 GDPR. |
| | *Ожидания* | • Уведомление о защите данных включает всю соответствующую контактную информацию, например, название и контактные данные организации (и её представителя, если это применимо) и контактные данные DPO.<br>• Уведомление о защите данных включает цели обработки и законные основания (и, если применимо, законные интересы для обработки). |

| | | |
|---|---|---|
| | | • Уведомление о защите данных включает типы ПД, которые организация получает, и источник данных, если ПД не получены от физического лица, к которому они относятся.<br>• Уведомление о защите данных включает сведения обо всех ПД, которыми организация делится с другими организациями, и, если это применимо, сведения о передаче ПД в любые третьи страны или международные организации.<br>• Уведомление о защите данных включает описание сроков хранения ПД или, если это невозможно, критерии, используемые для определения таких сроков.<br>• Уведомление о защите данных включает подробную информацию о правах субъектов данных, включая, если это применимо, право отозвать согласие и право подать жалобу.<br>• Уведомление о защите данных включает сведения о том, несут ли субъекты данных предусмотренное законом или контрактом обязательство предоставлять ПД (если это применимо, и если организация получает ПД от субъекта, к которому они относятся).<br>• Организация предоставляет субъектам данных информацию, касающуюся источника обрабатываемых ПД, если они получены из общедоступных источников, таких как социальные сети, открытый реестр избирателей или Регистрационная палата. |
| | *Ссылки* | • GDPR: ст.12-14; rc.58-59, 61-64<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on the Right of access (Information Commissioner's Office, October 2020) |
| 5.2 | *Контроль* | **Своевременное уведомление о защите данных** |
| | *Описание* | В организации есть формализованная процедура, позволяющая убедиться в том, что субъекты данных получают уведомление о защите данных в надлежащее время, если только не применяется исключение. |
| | *Ожидания* | • Субъекты данных получают уведомление о защите данных, когда собираются их данные (например, когда они заполняют форму) или путем наблюдения (например, при использовании систем видеонаблюдения или слежения за пользователями в интернете).<br>• Если организация получает ПД из источника, отличного от субъекта данных, к которому они относятся, она предоставляет уведомление о защите данных субъектам данных не позднее чем через месяц после получения данных. |
| | *Ссылки* | • GDPR: ст.12-14; rc.58-59, 61-64<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01 |
| 5.3 | *Контроль* | **Эффективное уведомление о защите данных** |
| | *Описание* | Организация предоставляет уведомление о защите данных, которое является:<br>кратким, прозрачным, доходчивым, понятным, написанным простым языком, сообщается таким образом, который эффективен для целевой аудитории. |
| | *Ожидания* | • Организация активно информирует субъектов о защите их данных и предоставляет им бесплатный и простой способ доступа к ним.<br>• Организация предоставляет уведомление о защите данных субъектам данных в электронной и печатной форме, используя комбинацию соответствующих методов, таких как многоуровневый подход, иконки и функциональные возможности мобильных и других смарт-устройств.<br>• Организация формулирует уведомление о защите данных ясным и понятным языком, который будет понятен целевой аудитории, и при необходимости предоставляет его в доступных форматах.<br>• Организация уделяет особое внимание написанию уведомления о защите данных для детей ясным, понятным языком, понятным для их возраста, и объясняет риски, связанные с обработкой, а также существующие меры защиты данных. |
| | *Ссылки* | • GDPR: ст.12-14; rc.58-59, 61-64<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01 |
| 5.4 | *Контроль* | **Уведомление об автоматизированных решениях и профилировании** |
| | *Описание* | Организация прозрачна в отношении любой обработки данных, связанной с автоматизированным принятием решений и профилированием. |
| | *Ожидания* | • В организации есть процедуры, позволяющие субъектам данных получать доступ к ПД, которые организация использует для создания профилей, чтобы субъекты могли проверить точность таких профилей и, при необходимости, запросить внесение в них изменений.<br>• Если решение полностью автоматизировано и имеет юридические или аналогичные существенные последствия, организация сообщает субъектам данных об обработке данных, в том числе о том, какие ПД она использует, по какой причине и каковы возможные последствия.<br>• Если цель изначально неясна, организация дает субъектам данных представление о том, что собирается делать с их данными, и активно обновляет уведомление о защите данных по мере прояснения цели обработки ПД.<br>• Если решение полностью автоматизировано и имеет юридические или аналогичные существенные последствия, организация объясняет обработку понятным для субъекта данных образом, который позволяет субъектам реализовать свои права, включая право на вмешательство человека, выражение своей точки зрения и оспаривание решения. |
| | *Ссылки* | • GDPR: ст.13-14, 22; rc.61-63, 71-72<br>• EDPB Guidelines 08/2020 on the targeting of social media users<br>• EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on use of cookies (Agencia Española de Protección de Datos, January 2021)<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Guidance on Cookies and Similar Technologies (Data Protection Commission, April 2020) |
| 5.5 | *Контроль* | **Осведомленность персонала** |
| | *Описание* | Организация может продемонстрировать, что любой сотрудник первой линии способен коммуницировать субъектам данных уведомление о защите данных и предоставить необходимые пояснения (рекомендации). |
| | *Ожидания* | • Организация организует обучение персонала по вопросам защиты данных и коммуникации уведомлений о защите данных.<br>• Персонал первой линии проходит более специализированное или специальное обучение в отношении уведомлений о защите данных.<br>• Персонал осведомлен о различных способах, с помощью которых организация предоставляет уведомление о защите данных. |

| | | |
|---|---|---|
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 5.6 | *Контроль* | **Пересмотр уведомлений о защите данных** |
| | *Описание* | В организации существуют процедуры для регулярного пересмотра уведомлений о защите данных, предоставляемых субъектам данных, чтобы гарантировать их точность, актуальность и эффективность. |
| | *Ожидания* | • Организация проверяет уведомления о защите данных в соответствии с записями о деятельности по обработке ПД, чтобы убедиться в их актуальности и наличии четкого описания процесса обработки ПД.<br>• Организация ведет учет прежних редакций уведомлений о защите данных, включая даты внесения изменений, чтобы можно было просмотреть, какое уведомление о защите данных организация предоставила субъектам данных и когда.<br>• Организация проводит тестирование уведомлений о защите данных на фокус-группах субъектов данных для оценки эффективности.<br>• Организация анализирует жалобы субъектов на обработку их данных, и, в частности, любые жалобы на то, как организация объясняет эту обработку.<br>• Если организация планирует обрабатывать ПД в новых целях, должна быть утверждена процедура обновления уведомлений о защите данных и доведения изменений до сведения субъектов данных до начала новой обработки. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 5.7 | *Контроль* | **Инструменты обеспечения прозрачности и контроля** |
| | *Описание* | Организация открыто сообщает о том, как обрабатывает ПД, и предлагает инструменты для обеспечения прозрачности и контроля, особенно при обработке ПД детей. |
| | *Ожидания* | • Политики защиты данных понятны и легкодоступны для субъектов данных.<br>• Организация предоставляет субъектам данных такие инструменты, как безопасные системы самообслуживания, информационные панели и своевременные уведомления, чтобы они могли получить доступ, определить и управлять тем, как организация использует их ПД.<br>• Организация предлагает строгие настройки защиты данных по умолчанию, а также удобные для пользователя опции и элементы управления.<br>• В соответствующих случаях, в организации имеются процессы, помогающие детям реализовать свои права на защиту данных в доступной и понятной для них форме.<br>• Организация принимает соответствующие меры для защиты детей, пользующихся цифровыми сервисами. |
| | *Ссылки* | • GDPR: ст.12-14; rc.58-59, 61-64<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01<br>• Guidelines on use of cookies (Agencia Española de Protección de Datos, January 2021)<br>• Guidance on Cookies and Similar Technologies (Data Protection Commission, April 2020) |

### 6. RoPA и законное основание

Документирование деятельности по обработке данных является требованием закона. Анализ того, какой информацией организация располагает, где она находится, и что организация с ней делает, значительно облегчает совершенствование управление и практическую реализацию защиты данных (например, создание уведомления о защите данных и обеспечение безопасности ПД). Это наглядный способ показать, что организация делает в соответствии с принципом отчетности, и SA могут потребовать, чтобы организация предоставляли им эти записи. Обработка ПД не будет законной без действительного законного основания, поэтому организация должна соответствующим образом обосновать свой выбор такого основания.

| | | |
|---|---|---|
| 6.1 | *Контроль* | **Сопоставление данных** |
| | *Описание* | Организация часто проводит комплексные мероприятия по составлению карт данных (data mapping), обеспечивая четкое понимание того, какие ПД хранятся и где. |
| | *Ожидания* | • Организация проводит информационные аудиты (или мероприятия по картированию данных), чтобы выяснить, какие ПД хранятся, и понять, как ПД циркулируют в организации.<br>• Организация поддерживает сведения о картах данных в актуальном состоянии и четко распределяет обязанности по их поддержанию и актуализации.<br>• Организация коммуницирует со своим персоналом (например, с помощью анкет и опросов), чтобы убедиться в наличии точного и актуального представления о деятельности по обработке данных. |
| | *Ссылки* | • GDPR: ст.30; rc.13, 39, 82<br>• Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 6.2 | *Контроль* | **Ведение RoPA** |
| | *Описание* | В организации имеется формальный, документированный, всеобъемлющий и точный RoPA, основанный на практике сопоставления данных, который регулярно пересматривается. |
| | *Ожидания* | • Организация фиксирует описание своей деятельности по обработке ПД в электронной форме, чтобы можно было легко добавлять, удалять и изменять информацию.<br>• Организация регулярно пересматривает реестр в отношении деятельности по обработке данных, политик и процедур, чтобы обеспечить его точность и актуальность, и организация четко распределяет обязанности персонала, связанные с этим.<br>• Организация регулярно пересматривает свою деятельность по обработке ПД и состав обрабатываемых данных в целях их минимизации. |
| | *Ссылки* | • GDPR: ст.30; rc.13, 39, 82 |
| 6.3 | *Контроль* | **Требования к RoPA** |
| | *Описание* | RoPA соответствует всем требованиям, изложенным в ст.30 GDPR. |
| | *Ожидания* | • RoPA должен включать (как минимум) следующую информацию:<br>- название и контактные данные организации, является ли она контролёром или лицом, обрабатывающим данные (и, если это применимо, совместный контролёр, его представитель и DPO);<br>- цели обработки;<br>- описание категорий субъектов данных и ПД;<br>- категории получателей ПД; |

| | | |
|---|---|---|
| | | - подробная информация о передаче в третьи страны, включая информацию о действующих гарантиях механизма передачи;<br>- срок хранения ПД;<br>- описание действующих технических и организационных мер безопасности.<br>• В организации есть внутренний реестр всех операций по обработке ПД, выполняемых любыми лицом, обрабатывающим данные от имени организации. |
| | *Ссылки* | • GDPR: ст.30<br>• Guidelines on record of processing activities (Commission Nationale de l'Informatique et des Libertés, August 2019)<br>• Registro delle attività di trattamento (Garante per la protezione dei dati personali, Ottobre 2018)<br>• Guidelines on record of processing activities (Information Commissioner's Office, September 2018) |
| 6.4 | *Контроль* | **Надлежащая практика для RoPA** |
| | *Описание* | RoPA организации содержит ссылки на другую соответствующую документацию, такую как соглашения или записи, в соответствии с требованиями надлежащей практики. |
| | *Ожидания* | • RoPA также включает документацию или ссылки на нее, охватывающую:<br>- информацию, необходимую для уведомлений о защите данных, такую как законное основание для обработки и источник ПД;<br>- записи о согласиях субъектов данных;<br>- соглашения между контролёром и лицом, обрабатывающим данные;<br>- местонахождение ПД;<br>- отчеты DPIA;<br>- записи о нарушении безопасности ПД;<br>- информацию, необходимую для обработки данных особой категории или данных о судимости и преступлениях;<br>- документы политик хранения и уничтожения ПД. |
| | *Ссылки* | • GDPR: ст.30<br>• Guidelines on record of processing activities (Commission Nationale de l'Informatique et des Libertés, August 2019)<br>• Registro delle attività di trattamento (Garante per la protezione dei dati personali, Ottobre 2018)<br>• Guidelines on record of processing activities (Information Commissioner's Office, September 2018) |
| 6.5 | *Контроль* | **Документирование законных оснований обработки данных** |
| | *Описание* | Организация документирует и надлежащим образом обосновывает законные основания для обработки ПД в соответствии со ст.6, 9-10 GDPR. |
| | *Ожидания* | • Организация выбирает наиболее подходящее законное основание (или основания) для каждого вида деятельности после анализа целей обработки.<br>• Организация документирует законное основание (или основания), на которое опирается при обработке ПД, и причины выбора такого основания.<br>• Если организация обрабатывает данные особой категории или данные о судимостях и правонарушениях, она определяет и документирует законное основание для общей обработки и дополнительное условие для обработки данных такого типа (или, в случае данных о судимостях и правонарушениях, организация указываете официальные полномочия для обработки).<br>• В случае обработки данных особой категории или данных о судимостях и правонарушениях организация документирует соблюдение требований ст.9 или 10 GDPR.<br>• Организация определяет законное основание перед началом любой новой обработки ПД. |
| | *Ссылки* | • GDPR: ст.6, 9-10; rc.40-56, 155<br>• Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data<br>• EDPB Guidelines 08/2020 on the targeting of social media users<br>• EDPB Guidelines 05/2020 on consent under Regulation 2016/679<br>• EDPB Guidelines 3/2019 on Processing of Personal Data through Video Devices<br>• EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects<br>• EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (December 2019)<br>• Opinion 2/2017 on data processing at work, WP249<br>• Guidance on Legal Bases for Data Processing (Data Protection Commission, December 2019) |
| 6.6 | *Контроль* | **Прозрачность законных оснований обработки данных** |
| | *Описание* | Организация делает информацию о целях обработки и законном основании общедоступной. Ее легко найти, открыть и прочитать. |
| | *Ожидания* | • Организация предоставляет информацию о целях обработки, законном основании и соответствующих условиях обработки ПД в открытом доступе в уведомлении(ях) о защите данных.<br>• Организация предоставляет информацию в легко понятном формате.<br>• Если обстоятельства изменились или если ваше законное основание должно измениться в связи с новой и непредвиденной задачей, организация своевременно информирует об этом субъектов данных и регистрируете изменения. |
| | *Ссылки* | • GDPR: ст.12; rc.58-59, 64<br>• Guidelines on transparency under Regulation 2016/679, WP260 rev.01 |
| 6.7 | *Контроль* | **Требования к согласию** |
| | *Описание* | Если организация подучает у субъектов согласие на обработку их данных, то оно должно быть: конкретным; детализированным; наглядным; добровольным; задокументированным; легко отзываемым. |
| | *Ожидания* | • Запросы на получение согласия:<br>- хранятся отдельно от других положений и условий взаимодействия между организацией и субъектом данных;<br>- требуют утвердительного ответа субъекта данных и не используют предварительно установленные флажки;<br>- являются четкими и конкретными (не являются предварительным условием регистрации в сервисе);<br>- информируют субъектов данных о способе простого отзыва согласия;<br>- указывают название организации, а также любых третьих лиц, использующих согласие. |

| | | |
|---|---|---|
| | | • В организации есть записи о том, на что субъект данных предоставил свое согласие, в том числе о том, что ему было сказано, когда и как было получено согласие. Записи являются подробными, и соответствующий персонал может легко получить к ним доступ, просмотреть их и исключить при необходимости.<br>• В организации есть доказательства и примеры того, как запрашивается согласие у субъектов данных, например, онлайн-формы или уведомления, флажки для выбора варианта или бумажные формы. |
| | *Ссылки* | • GDPR: ст.7; rc.32-33, 42-43<br>• EDPB Guidelines 05/2020 on consent under Regulation 2016/679<br>• Guidelines on use of cookies (Agencia Española de Protección de Datos, January 2021)<br>• Guidance on Cookies and Similar Technologies (Data Protection Commission, April 2020) |
| 6.8 | *Контроль* | **Пересмотр согласия** |
| | *Описание* | Организация активно просматриваете записи о ранее полученных согласиях, что демонстрирует приверженность подтверждению и обновлению согласий. |
| | *Ожидания* | • В организации есть процедура проверки согласий, позволяющая удостовериться, что отношения, обработка и цели не изменились, и зарегистрировать любые изменения.<br>• В организации существует процедура обновления согласия через соответствующие промежутки времени.<br>• Организация использует панели мониторинга защиты данных (privacy dashboards) или другие инструменты управления предпочтениями, чтобы помочь людям управлять своим согласием. |
| | *Ссылки* | • GDPR: ст.7; rc.32-33, 42-43<br>• EDPB Guidelines 05/2020 on consent under Regulation 2016/679 |
| 6.9 | *Контроль* | **Проверка возраста с учетом риска и согласие родителей или опекунов** |
| | *Описание* | В организации существуют эффективные системы для проведения проверок возраста субъектов данных с учетом риска и, при необходимости, для получения и регистрации согласия родителей или опекунов субъектов данных. |
| | *Ожидания* | • Организация прилагает разумные усилия для проверки возраста субъектов данных, дающих согласие, особенно если это ребенок.<br>• В организации есть разумная и эффективная процедура для определения того, может ли данное лицо предоставить свое собственное согласие, а если нет, то эффективный способ получить и зарегистрировать согласие родителей или опекунов.<br>• При предоставлении онлайн-услуг детям организация имеет системы проверки возраста с учетом оценки рисков, позволяющие установить возраст с соответствующим уровнем достоверности, исходя из рисков для прав и свобод детей.<br>• При предоставлении онлайн-услуг детям, если ребенок младше 16 лет, в организации есть записи о согласии родителей или опекунов, которые регулярно проверяются, и организация прилагает разумные усилия для проверки того, что лицо, дающее согласие, несет родительскую ответственность.<br>• Организация уделяет особое внимание ситуации, когда ребенок достигает 16-летнего возраста и может дать собственное согласие. |
| | *Ссылки* | • GDPR: ст.8; rc.38<br>• EDPB Guidelines 05/2020 on consent under Regulation 2016/679<br>• Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP160<br>• Age Appropriate Design: A Code of Practice for Online Services (Information Commissioner’s Office, August 2021)<br>• Data Protection Commissioner/Facebook Ireland Ltd and Schrems, C-311/18 (Court of Justice of the European Union, July 2020) |
| 6.10 | *Контроль* | **LIA** |
| | *Описание* | Если законной основой организации являются законные интересы, организация выполнила соответствующую LIA до начала обработки данных. |
| | *Ожидания* | • LIA определяет законный интерес, преимущества обработки данных и необходимость в ней.<br>• LIA включает «проверку на сбалансированность» для демонстрации того, что ее законные интересы превышают интересы субъектов данных, и учитывает следующие аспекты:<br>- отсутствие факта использования данных субъектов навязчивыми способами или способами, которые могут нанести им вред, если на то нет очень веских причин;<br>- защита интересов уязвимых групп субъектов данных, таких как люди с ограниченными возможностями обучения или дети;<br>- есть ли у организации возможность ввести меры предосторожности для уменьшения любого потенциально негативного воздействия на субъектов данных;<br>- может ли организация предложить субъектам возможность отказа от обработки их данных (opt-out);<br>- требуется ли осуществление DPIA.<br>• Организация четко документирует решение и оценку законного интереса.<br>• Организация выполняет LIA до начала обработки данных.<br>• Организация пересматриваете LIA и обновляете ее, если изменения влияют на результат. |
| | *Ссылки* | • GDPR: ст.6; rc.47-49<br>• EDPB Guidelines 08/2020 on the targeting of social media users<br>• Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217<br>• Guidelines on Legitimate interests (Information Commissioner’s Office, January 2021)<br>• TK v Asociaţia de Proprietari bloc M5A-ScaraA, Case C-708/18 (Court of Justice of the European Union, December 2019) |

### 7. Соглашения и обмен данными

Хорошей практикой является заключение письменных соглашений о совместном использовании данных, когда контролёры обмениваются ПД. Это помогает каждому понять цель обмена данными, процессов, которые будут происходить на каждом этапе, и своих обязанностей. Это также поможет организации продемонстрировать соответствие требованиям в четкой и формальной форме. Аналогичным образом, письменные соглашения помогают контролёрам и лицам, обрабатывающим данные, продемонстрировать соблюдение требований и понять свои обязательства, функции и ответственность.

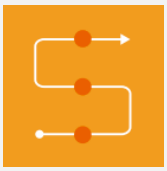
| | | |
|---|---|---|
| 7.1 | *Контроль* | **Политики и процедуры обмена данными** |
| | *Описание* | Политики и процедуры организации гарантируют, что организация надлежащим образом управляет своими решениями об обмене данными. |

| | | |
|---|---|---|
| | *Ожидания* | • В организации есть процесс анализа с помощью DPIA или аналогичного метода для оценки законности, преимуществ и рисков обмена данными.<br>• Организация документирует все решения об обмене данными в целях аудита, мониторинга и расследования и регулярно просматривает их.<br>• В организации действуют четкие политики, процедуры и рекомендации по обмену данными, в том числе о том, кто уполномочен принимать решения о систематическом обмене данными или разовом раскрытии данных, и когда это уместно.<br>• Организация надлежащим образом обучает персонал, который может принимать решения об обмене данными, и информирует его о соответствующих обязанностях. Организация своевременно обновляет это обучение. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 7.2 | *Контроль* | **Соглашения об обмене данными** |
| | *Описание* | Организация заключает и регулярно пересматривает соглашения об обмене данными (Controller-to-Controller & Joint Controllers agreements) со сторонами, с которыми организация регулярно делится ПД. |
| | *Ожидания* | • Организация согласовывает соглашения об обмене данными со всеми соответствующими сторонами, а руководство организации подписывает их.<br>• Соглашение об обмене данными включает подробную информацию о:<br>- функциях сторон;<br>- целях обмена данными;<br>- том, что будет происходить с данными на каждом этапе их обработки;<br>- установленных стандартах защиты данных (с высоким уровнем защиты данных детей по умолчанию).<br>• При необходимости, процедуры и руководства, охватывающие повседневную деятельность каждой организации, поддерживают нормы соглашений.<br>• Если организация действует в качестве совместного контролёра (по смыслу ст.26 GDPR), она устанавливает обязанности в соответствии с договоренностью или соглашением об обмене данными и предоставляет соответствующую уведомление о защите данных субъектам данных.<br>• В организации есть процесс регулярного контроля, позволяющий удостовериться в том, что ПД остаются точными и актуальными, а также проанализировать исполнение соглашения.<br>• Организация ведет централизованный учет заключённых соглашений об обмене данными. |
| | *Ссылки* | • GDPR: ст.26; rc.79<br>• EDPB Guidelines 04/2021 on codes of conduct as tools for transfers<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Tietosuojavaltuutettu, C-25/17 (Court of Justice of the European Union, July 2018)<br>• Wirtschaftsakademie Schleswig-Holstein, C-210/16 (Court of Justice of the European Union, June 2018) |
| 7.3 | *Контроль* | **Трансграничная передача данных** |
| | *Описание* | В организации действуют процедуры, позволяющие гарантировать, что трансграничная передача данных (restricted data transfer) осуществляются надлежащим образом. |
| | *Ожидания* | • Организация решает, покрывается ли трансграничная передача данных решениями об адекватности (ст.45 GDPR) или надлежащими гарантиями (ст.46 GDPR), такими как SCC или BCR.<br>• Если трансграничная передача данных не подпадает под действие решений об адекватности или надлежащих гарантий, организация должна рассмотреть вопрос о применимости исключений из ст.49 GDPR. |
| | *Ссылки* | • GDPR: ст.44-49; rc.101-115<br>• EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR<br>• EDPB Guidelines 04/2021 on codes of conduct as tools for transfers<br>• EDPB Guidelines 02/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies<br>• EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data<br>• EDPB Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679<br>• Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679<br>• Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265<br>• Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP 263 rev.01<br>• Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264<br>• Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01<br>• Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01<br>• Explanatory Document on the Processor Binding Corporate Rules, WP 204 rev.01<br>• Guidelines on International Transfers (Information Commissioner's Office, January 2021)<br>• Data Protection Commissioner/Facebook Ireland Ltd and Schrems, C-311/18 (Court of Justice of the European Union, July 2020) |
| 7.4 | *Контроль* | **Процессоры** |
| | *Описание* | В организации есть соответствующие процедуры, обработки данных, которую процессоры выполняют от имени организации. |
| | *Ожидания* | • В организации есть письменные соглашения (Controller-to-Processor agreement) со всеми процессорами.<br>• При привлечении процессора организация оценивает риски для субъектов данных и гарантирует эффективное снижение этих рисков.<br>• Соответствующие руководители организации утверждают соглашения, и обе стороны подписывают их. Уровень руководства организации, необходимый для утверждения соглашения, пропорционален важности и рискам соглашения. |

| | | |
|---|---|---|
| | | • В каждом соглашении (или другом правовом акте) излагаются детали обработки, в том числе:<br>- предмет обработки;<br>- продолжительность обработки;<br>- характер и цель обработки;<br>- категории обрабатываемых данных;<br>- категории субъектов данных;<br>- обязанности и права контролёра в соответствии с перечнем из ст.28(3) GDPR.<br>• Организация ведет учет всех заключенных соглашений с процессорами, и актуализирует учетную документацию при их смене.<br>• Организация периодически просматривает соглашения, чтобы гарантировать их актуальность.<br>• Если процессор использует субподрядчика для содействия в обработке данных, выполняемой от имени организации, у него должно быть письменное разрешение от организации и письменное соглашение с таким субподрядчиком. |
| | *Ссылки* | • GDPR: ст.28-29; rc.81<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles (Commission Nationale de l'Informatique et des Libertés, Juillet 2020)<br>• A Practical Guidelines to Controller-Processor Contracts (Data Protection Commission, June 2019)<br>• Guidelines for Processors (Commission Nationale de l'Informatique et des Libertés, September 2017) |
| 7.5 | *Контроль* | **Требования к соглашению между контролёром и процессором** |
| | *Описание* | Все соглашения (Controller-to-Processor agreements) между контролёром и процессором охватывают условия и положения, необходимые для соблюдения GDPR. |
| | *Ожидания* | • Соглашение или другой правовой акт содержит условия или положения, в которых указывается, что процессор должен:<br>- действовать только в соответствии с документированными инструкциями контролёра, если только закон не требует действовать без таких инструкций;<br>- гарантировать, что персонал, обрабатывающий данные, соблюдает требования к защите данных;<br>- помогать контролёру отвечать на запросы субъектов данных о реализации их прав;<br>- проходить аудит и проверки со стороны контролёра.<br>• Соглашения включают технические и организационные меры безопасности, которые должен соблюдать процессор (включая шифрование, псевдонимизацию, устойчивость систем обработки и резервное копирование ПД для обеспечения возможности их восстановления).<br>• В соглашение включаются положения, гарантирующие, что процессор либо удалит, либо вернет все ПД контролёру по окончании срока действия контракта. Процессор также должен удалить существующие ПД, если только закон не требует их хранения.<br>• Соглашение включает положения, гарантирующие, что процессор помогает контролёру в выполнении его обязательств по GDPR в отношении безопасности обработки ПД, уведомления о нарушениях безопасности ПД и DPIA. |
| | *Ссылки* | • GDPR: ст.28-29, 32; rc.77, 81, 83<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Commission implementing decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles Commission Nationale de l'Informatique et des Libertés, Juillet 2020)<br>• A Practical Guidelines to Controller-Processor Contracts (Data Protection Commission, June 2019)<br>• Guidelines for Processors (Commission Nationale de l'Informatique et des Libertés, September 2017) |
| 7.6 | *Контроль* | **Проверка добросовестности процессора** |
| | *Описание* | Организация проводит проверки добросовестности процессоров, чтобы гарантировать применение ими соответствующих технических и организационных мер защиты данных в соответствии с требованиями GDPR. |
| | *Ожидания* | • Процесс закупок включает в себя проверку добросовестности, соразмерную риску обработки данных, выполняемую до согласования соглашения с процессором.<br>• Процесс проверки добросовестности включает проверки безопасности данных, например, посещения сайтов, запросы на тестирование системы и аудит.<br>• Процесс проверки добросовестности включает проверки для подтверждения того, что потенциальный процессор будет защищать права субъектов данных. |
| | *Ссылки* | • GDPR: ст.28, 32; rc.77, 81, 83<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles Commission Nationale de l'Informatique et des Libertés, Juillet 2020) |
| 7.7 | *Контроль* | **Проверки соблюдения требований процессором** |
| | *Описание* | Организация проверяет соблюдение требований соглашения процессорами. |
| | *Ожидания* | • Соглашения включают положения, позволяющие организации проводить аудиты или проверки, чтобы подтвердить, что процессор соблюдает все договорные условия и положения.<br>• Организация проводит регулярные проверки соблюдения требований, пропорциональные рискам обработки данных, чтобы проверить, соблюдаются ли договорные соглашения процессорами. |
| | *Ссылки* | • GDPR: ст.28, 32; rc.77, 81, 83<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles Commission Nationale de l'Informatique et des Libertés, Juillet 2020) |

| | | |
|---|---|---|
| 7.8 | *Контроль* | **Продукты и услуги третьих лиц** |
| | *Описание* | Организация практикует принцип «проектируемой защиты данных» при выборе услуг и продуктов для использования в своей деятельности по обработке данных. |
| | *Ожидания* | • Когда третьи лица поставляют свои продукты или услуги для обработки ПД, организация выбираете поставщиков, которые разрабатывают свои продукты или услуги с учетом принципа «проектируемой защиты данных». |
| | *Ссылки* | • GDPR: ст.25, 28; rc.78<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles Commission Nationale de l'Informatique et des Libertés, Juillet 2020) |
| 7.9 | *Контроль* | **Ограничение передачи данных целью** |
| | *Описание* | Организация активно предпринимает шаги для обмена с процессорами или другими третьими лицами только необходимыми ПД. |
| | *Ожидания* | • Организация предоставляет процессорам и иным третьим лицам только такие ПД, которые необходимые для достижения конкретной цели.<br>• При передаче данных они, по возможности, псевдонимизируются или минимизируются. Организация также рассматривает возможность анонимизации данных, чтобы передаваемые данные больше не представляли собой ПД. |
| | *Ссылки* | • GDPR: ст.25, 28; rc.78<br>• EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Responsable de traitement et sous-traitant: 6 bonnes pratiques pour respecter les données personnelles Commission Nationale de l'Informatique et des Libertés, Juillet 2020) |
| 7.10 | *Контроль* | **Определение необходимости и назначение представителя** |
| | *Описание* | Если организация не имеет учреждения в ЕЕА (представительства, филиалы, дочерние предприятия, сотрудники), но осуществляет обработку данных, соответствующую критериям ст.3 GDPR, то она должна назначить представителя, за исключением некоторых случаев. |
| | *Ожидания* | • Обоснование наличия или отсутствия необходимости назначения организацией своего представителя в ЕЕА документировано, сообщено руководству организации и подтверждено им.<br>• Осуществлено удостоверение факта учреждения представителя в одном из государств-членов ЕЕА, где находятся субъекты, данные которых обрабатываются в контексте требований GDPR.<br>• Представитель должен быть в явной форме уполномочен, посредством письменного предписания организации (например, доверенности), действовать от имени организации в отношении её обязанностей по GDPR. |
| | *Ссылки* | • GDPR: ст.27; rc.80<br>• Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, WP248 rev.01 |

## 8. Оценка рисков и DPIA



Необходимость выявления, оценки и управления рисками защиты данных является неотъемлемой частью принципа подотчетности. Понимание рисков, связанных с тем, как организация использует ПД, имеет решающее значение для создания надлежащей и пропорциональной системы управления защитой данных. DPIA – это ключевой инструмент управления рисками и важная часть интеграции подхода DPDD в организации. DPIA помогает организации выявлять, регистрировать и минимизировать риски защиты данных в её проектах. В некоторых случаях проведение DPIA является обязательным, и существуют особые юридические требования к содержанию и процессу DPIA. Если организация не может снизить высокий риск для защиты данных, она должна установить порядок уведомления SA об этом.

| | | |
|---|---|---|
| 8.1 | *Контроль* | **Выявление, регистрация и управление рисками** |
| | *Описание* | В организации действует соответствующие политики, процедуры и меры для выявления, регистрации и управления рисками защиты данных. |
| | *Ожидания* | • Политика в области рисков защиты данных (либо отдельный документ, либо часть общей корпоративной политики в области рисков) определяет то, как организация и лица, обрабатывающие данные от ее имени, управляют рисками защиты данных, и как организация контролирует соблюдение политики в отношении таких рисков.<br>• В организации есть процесс, помогающий персоналу сообщать о проблемах и рисках, связанных с управлением и практической реализацией защиты данных, и передавать их в централизованную точку сбора таких сведений.<br>• Организация выявляет риски защиты данных и управляет ими посредством соответствующего реестра рисков, который включает четкие связи между корпоративными и ведомственными реестрами рисков и оценкой рисков в отношении информационных активов.<br>• В организации есть официальные процедуры для определения, регистрации и управления рисками в отношении информационных активов, зафиксированных в реестре таких активов.<br>• Если организация выявляет риски защиты данных, она реализует планы реагирования, фиксирует отчеты о проделанной работе и о рассмотрении извлеченных уроков, чтобы избежать рисков в будущем.<br>• Организация принимает меры для снижения выявленных рисков защиты данных и регулярно проверяет их, чтобы гарантировать их эффективность. |
| | *Ссылки* | • GDPR: ст.24; rc.74-77, 83<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 8.2 | *Контроль* | **DPIA как элемент DPDD** |
| | *Описание* | Организация использует подход к управлению рисками, основанный на подходе DPDD, и, при необходимости, включает требования о проведении DPIA в свои политики и процедуры. |
| | *Ожидания* | • Организация указывает на требование о проведении DPIA во всех политиках и процедурах управления рисками, проектами и изменениями со ссылками на политику и процедуры DPIA. |

| | | |
|---|---|---|
| | | • В политиках и процедурах организации указано, что DPIA должна проводиться с самого начала проекта, до начала обработки данных, и что DPIA должна проводиться параллельно с процессом планирования и разработки.<br>• Организация предвидит риски и события, нарушающие защиту данных, до их возникновения, следя за тем, чтобы на начальном этапе проектирования любой системы, продукта или процесса, а также на протяжении всего процесса учитывались следующие факторы:<br>- предполагаемая деятельность по обработке данных;<br>- риски, которые они могут представлять для прав и свобод субъектов данных;<br>- возможные меры, доступные для снижения рисков. |
| | *Ссылки* | • GDPR: ст.25; rc.78<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020)<br>• A Guidelines to Privacy by Design (Agencia Española de Protección de Datos, October 2019) |
| 8.3 | *Контроль* | **Политики и процедуры DPIA** |
| | *Описание* | Организация понимает, требуется ли проведение DPIA, и когда ее проведение было бы целесообразным. Существует четкая политика и процедура DPIA. |
| | *Ожидания* | • В организации есть политика DPIA, которая включает в себя:<br>- четкие процедуры для принятия решения о том, следует ли проводить DPIA;<br>- что должна охватывать DPIA;<br>- кто дает разрешение на проведение DPIA;<br>- как организация будет включать DPIA в общее планирование своей деятельности.<br>• В организации есть контрольный список (чек-лист) для рассмотрения вопроса о необходимости проведения DPIA, включая все соответствующие соображения относительно объема, типа и способа предлагаемой обработки ПД.<br>• Если, согласно контрольному списку, нет необходимости в проведении DPIA, организация документирует это решение.<br>• Процедуры организации включают в себя требование обратиться за консультацией по поводу проведения DPIA к DPO и к другому уполномоченному персоналу, если это необходимо.<br>• Процедуры организации включают в себя консультации с контролёрами, процессорами, субъектами данных, их представителями и любыми другими заинтересованными сторонами, если это необходимо.<br>• Обучение персонала включает в себя информирование о необходимости проведения DPIA на ранних стадиях любого проекта, связанного с обработкой ПД, и, при необходимости, организация обучает персонал тому, как проводить DPIA.<br>• Организация возлагает ответственность за проведение DPIA на сотрудника, который обладает достаточными полномочиями в отношении проекта для внесения в него изменений (корреткировок), например, на руководителя проекта или менеджера. |
| | *Ссылки* | • GDPR: ст.35; rc.75, 84, 89-93<br>• Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, WP248 rev.01<br>• Gestión del riesgo y evaluación de impacto en tratamientos de datos personales' (Agencia Española de Protección de Datos, Junio de 2021)<br>• Guidelines on Data protection impact assessments (Information Commissioner's Office, January 2021)<br>• Guide to Data Protection Impact Assessments (Data Protection Commission, October 2019)<br>• Guidelines on Privacy Impact Assessment (Commission Nationale de l'Informatique et des Libertés, February 2018) |
| 8.4 | *Контроль* | **Содержание DPIA** |
| | *Описание* | DPIA всегда содержит соответствующую информацию и должен быть всесторонне документирован. |
| | *Ожидания* | • В организации есть стандартный, хорошо структурированный шаблон DPIA, написанный на простом языке.<br>• DPIA:<br>- описывает характер, объем, контекст и цели обработки данных;<br>- оценивает необходимость, соразмерность и меры по соблюдению требований к защите данных;<br>- выявляет и оценивает риски для субъектов данных;<br>- определяет любые дополнительные меры по снижению этих рисков.<br>• DPIA четко определяет взаимосвязи и потоки данных между контролёрами, процессорами, субъектами данных и системами.<br>• DPIA определяет меры для устранения, смягчения или снижения высоких рисков.<br>• В организации есть документированный процесс с соответствующими средствами управления документацией, который организация периодически пересматривает, чтобы гарантировать его актуальность.<br>• Организация фиксирует советы и рекомендации своего DPO, а также подробную информацию о любых других консультациях со стороны вовлеченных в DPIA лиц.<br>• Соответствующие лица, такие как руководитель проекта или старший менеджер, подписывают DPIA. |
| | *Ссылки* | • GDPR: ст.35; rc.75, 84, 89-93<br>• Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, WP248 rev.01<br>• Gestión del riesgo y evaluación de impacto en tratamientos de datos personales' (Agencia Española de Protección de Datos, Junio de 2021)<br>• Guidelines on Data protection impact assessments (Information Commissioner's Office, January 2021)<br>• Guide to Data Protection Impact Assessments (Data Protection Commission, October 2019)<br>• Guidelines on Privacy Impact Assessment (Commission Nationale de l'Informatique et des Libertés, February 2018) |
| 8.5 | *Контроль* | **Снижение рисков и проверка DPIA** |
| | *Описание* | Организация предпринимает надлежащие и эффективные действия для снижения или управления любыми рисками, выявленными при проведении DPIA, и в организации есть процесс проверки DPIA. |
| | *Ожидания* | • В организации есть процедура для консультации с SA, если организация не может снизить остаточные высокие риски в отношении защиты данных. |

| | | |
|---|---|---|
| | | • Организация интегрирует результаты DPIA в соответствующие рабочие планы, планы действий по проектам и реестры рисков.<br>• Организация не начинает обработку данных с высоким риском до тех пор, пока не будут приняты меры по смягчению последствий в соответствии с DPIA.<br>• В организации есть процедура для информирования соответствующих заинтересованных сторон о результатах DPIA, например, посредством официального сводного отчета.<br>• Организация рассматривает возможность публикации результатов DPIA для широкого круга лиц, если это возможно, удаляя конфиденциальные данные при необходимости.<br>• Организация утверждает и документирует график проверки DPIA на регулярной основе или при изменении характера, объема, контекста или целей обработки данных. |
| | *Ссылки* | • GDPR: ст.35-36; rc.75, 84, 89-96<br>• Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, WP248 rev.01<br>• Gestión del riesgo y evaluación de impacto en tratamientos de datos personales' (Agencia Española de Protección de Datos, Junio de 2021)<br>• Guidelines on Data protection impact assessments (Information Commissioner's Office, January 2021)<br>• Guide to Data Protection Impact Assessments (Data Protection Commission, October 2019)<br>• Guidelines on Privacy Impact Assessment (Commission Nationale de l'Informatique et des Libertés, February 2018) |

## 9. Управление записями и безопасность

Надлежащее управление записями способствует должному управлению данными и защите данных. К более широким преимуществам относятся обеспечение доступа к данным, уверенность в том, что организация сможет найти информацию о прошлой деятельности, и возможность более эффективного использования ресурсов. Некоторые из последствий неэффективного управления записями включают принятие неверных решений, неспособность безопасно работать с данными и неэффективность деятельности по обработке данных. ИБ также поддерживает эффективное управление данными, и сама по себе является юридическим требованием к защите данных. Низкий уровень ИБ подвергает риску системы и сервисы и может причинить реальный вред и страдания субъектам данных – в некоторых крайних случаях это может даже поставить под угрозу жизни людей.

| | | |
|---|---|---|
| 9.1 | *Контроль* | **Создание, поиск и получение записей** |
| | *Описание* | В организации есть минимальные стандарты для создания записей и эффективные механизмы для поиска и получения записей. |
| | *Ожидания* | • В организации есть политики и процедуры для обеспечения надлежащей классификации, наименования и индексации новых записей для облегчения управления, поиска и удаления таких записей.<br>• Организация определяет, где используются ручные и автоматизированные системы учета записей, и ведет централизованный журнал или реестр информационных активов.<br>• Организация всегда знает местонахождение записей, отслеживает их перемещения и старается отследить пропавшие или не возвращенные записи.<br>• Организация индексирует записи, хранящиеся за пределами ее мест расположения, с использованием уникальных идентификаторов для обеспечения точного поиска таких записей и последующего отслеживания. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 9.2 | *Контроль* | **Безопасность при передаче данных** |
| | *Описание* | В организации есть соответствующие меры безопасности для защиты данных, которые организация получает от других лиц и/или передает им. |
| | *Ожидания* | • Организация документирует правила для защиты внутренней и внешней передачи данных по почте, факсу и в электронном виде.<br>• Передача данных за пределы организации минимизирована, и обеспечена безопасность данных при их передаче.<br>• При передаче данных за пределы организация используется соответствующие способы (например, безопасный курьер, шифрование, протокол безопасной передачи файлов – SFTP или виртуальная частная сеть – VPN) и выполняется проверка факта получения данных надлежащим лицом.<br>• В организации есть действующие соглашения о защите данных со всеми поставщиками, которые используются для передачи данных между организацией и третьими лицами. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Data sharing: a code of practice (Information Commissioner's Office, December 2020)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 9.3 | *Контроль* | **Качество данных** |
| | *Описание* | В организации есть процедуры, обеспечивающие точность, адекватность и отсутствие избыточности записей, содержащих ПД. |
| | *Ожидания* | • Организация регулярно проводит проверку качества записей, содержащих ПД, чтобы убедиться, что они являются точными, адекватными и не избыточными.<br>• Организация информируете персонал о проблемах с качеством данных после проверок или аудитов качества данных, чтобы предотвратить их повторение.<br>• Записи, содержащие ПД (активные или архивированные), периодически проверяются («очищаются»), чтобы снизить риски неточностей и хранения чрезмерного объема данных. |
| | *Ссылки* | • GDPR: ст.25; rc.78<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020)<br>• A Guidelines to Privacy by Design (Agencia Española de Protección de Datos, October 2019) |
| 9.4 | *Контроль* | **Сроки хранения данных** |
| | *Описание* | В организации есть соответствующая процедура (Data Retention Policy) для определения сроков хранения ПД, которые организация регулярно пересматривает. |

| | | |
|---|---|---|
| | *Ожидания* | • В организации есть процедура для определения сроков хранения ПД исходя из потребностей бизнеса с учетом положений законодательства и иных требований.<br>• Процедура предоставляет достаточную информацию для идентификации всех записей с ПД и принятия решений об уничтожении данных в соответствии с утвержденным графиком.<br>• Организация распределяет обязанности среди персонала, чтобы гарантировать, соблюдение персоналом графика уничтожения ПД, и регулярно пересматривает такой график. Организация регулярно проверяет сохраненные данные, чтобы определить возможности для их минимизации, псевдонимизации или анонимизации, и документирует это в отчетных материалах. |
| | *Ссылки* | • GDPR: ст.25, 32; rc.74-78, 83<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020)<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• A Guidelines to Privacy by Design (Agencia Española de Protección de Datos, October 2019)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 9.5 | *Контроль* | **Уничтожение данных** |
| | *Описание* | Организация описывает методы уничтожения данных в своих политиках и процедурах, и они обеспечивают предотвращение раскрытия ПД до, во время и после их уничтожения. |
| | *Ожидания* | • Для бумажных документов, содержащих ПД, организация использует закрытые мусорные контейнеры, а также осуществляет измельчаете или сжигаете документов либо собственными силами, либо с привлечением третьих лиц.<br>• Для данных, хранящихся на электронных устройствах, должно быть предусмотрено стирание, размагничивание или безопасное уничтожение оборудования (измельчение).<br>• Организация обеспечивает безопасный процесс собора, хранения либо отправки третьим лицам материальных носителей с ПД, ожидающих уничтожения.<br>• Организацией заключены соответствующие соглашения с третьими лицами на утилизацию ПД, и они предоставляют организации соответствующие гарантии безопасной утилизации данных, например, посредством аудиторских проверок и сертификатов об уничтожении.<br>• В организации есть процедура регистрации всего оборудования и материальных носителей ПД, отправленных на утилизацию или уничтожение. |
| | *Ссылки* | • GDPR: ст.25, 32; rc.74-78, 83<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020)<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• A Guidelines to Privacy by Design (Agencia Española de Protección de Datos, October 2019)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 9.6 | *Контроль* | **Реестр информационных активов** |
| | *Описание* | В организации есть реестр информационных активов (IAR), в котором регистрируются информационные ресурсы, системы и приложения, используемые для обработки, в т.ч. хранения ПД, в организации. |
| | *Ожидания* | • В организации есть реестр, в котором содержатся подробные сведения обо всех информационных активах:<br>- владельцы активов;<br>- местоположение активов;<br>- сроки хранения данных;<br>- применяемые меры безопасности.<br>• Организация периодически пересматривает реестр, чтобы убедиться, что он остается актуальным и точным.<br>• Организация периодически проводит оценку рисков для активов в реестре и проводит физические проверки, чтобы гарантировать точность инвентаризации оборудования. |
| | *Ссылки* | • Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 9.7 | *Контроль* | **Правила допустимого использования программного обеспечения** |
| | *Описание* | Организация определяет, документирует и внедряет правила допустимого использования программного обеспечения (систем или приложений), используемого для обработки данных. |
| | *Ожидания* | • В организации есть процедуры, устанавливающие правила и условия допустимого использования программного обеспечения.<br>• В организации есть системные операционные процедуры, которые документируют механизмы и меры безопасности, применяемые для защиты данных, хранящихся в системах или приложениях.<br>• Организация следит за соблюдением правил допустимого использования и следит за тем, чтобы персонал был осведомлен о любом мониторинге использования им программного обеспечения. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018)<br>• Opinion 2/2017 on data processing at work, WP249 |
| 9.8 | *Контроль* | **Контроль доступа** |
| | *Описание* | Организация предоставляет доступ к ПД только уполномоченному персоналу и регулярно проверяет права доступа пользователей. |
| | *Ожидания* | • В организации есть политика контроля доступа, которая определяет обязанность пользователей следовать правилам организации при использовании секретной информации для аутентификации, например, паролей или уникальных кодов. |

| | | |
|---|---|---|
| | | • Организация внедряет официальную процедуру предоставления доступа пользователям для назначения прав доступа к системам и приложениям для персонала (включая временный персонал) и сторонних подрядчиков, которые необходимы им для выполнения соответствующих функций.<br>• Организация ограничивает и контролирует распределение и использование привилегированных прав доступа.<br>• Организация ведет журнал доступа пользователей к системам и приложениям, содержащим ПД.<br>• Организация регулярно проверяет права доступа пользователей и при необходимости корректирует или удаляет права, например, когда сотрудник меняет свою функцию или покидает организацию. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018)<br>• Opinion 2/2017 on data processing at work, WP249 |
| 9.9 | *Контроль* | Несанкционированный доступ |
| | *Описание* | Организация предотвращает несанкционированный доступ к системам и приложениям с ПД, например, с помощью паролей, средств управления техническими уязвимостями и предотвращения вредоносных программ. |
| | *Ожидания* | • Организация ограничивает доступ к системам или приложениям, обрабатывающим ПД, до абсолютного минимума в соответствии с принципом наименьших привилегий (например, применяются правила доступа для чтения/записи/удаления/выполнения).<br>• Организация применяет правила минимальной сложности пароля и ограничивает количество попыток входа в системы или приложения, обрабатывающие ПД.<br>• В организации есть средства управления паролями, включая изменение пароля по умолчанию, контролируемое использование любых общих паролей и безопасное хранение паролей (не в виде обычного текста).<br>• Решения для защиты содержимого электронной почты и вложений (шифрование) надлежащим образом защищают электронные письма, содержащие ПД.<br>• Организация регистрирует и отслеживает активность пользователей и систем для обнаружения любых необычных событий.<br>• Организация внедряет защиту от вредоносных программ и вирусов (AV) по всей сети и в системах с критически важной или конфиденциальной информацией, если это необходимо.<br>• Защита от вредоносных программ и вирусов поддерживается в актуальном состоянии, и организация настраивает ее для регулярного сканирования.<br>• Организация имеет доступ ко всем необходимым обновлениям для устанения технических уязвимостей систем или программного обеспечения, например, к предупреждениям или исправлениям производителей, и принимает соответствующие меры.<br>• Организация регулярно запускает сканирование уязвимостей.<br>• Организация применяет фильтрацию URL-адресов или веб-контента, чтобы блокировать определенные веб-сайты или целые категории.<br>• Организация строго контролирует или запрещает использование социальных сетей или мессенджеров, таких как WhatsApp, для обмена личными данными.<br>• В организации есть внешние и внутренние брандмауэры и системы обнаружения вторжений, необходимые для обеспечения безопасности информации в сетях и системах от несанкционированного доступа или атак, например атак типа «отказ в обслуживании».<br>• В организации не используются неподдерживаемые операционные системы, например Windows XP или Windows Server 2003.<br>• Организация устанавливает специальные средства контроля для обеспечения конфиденциальности и целостности данных, передаваемых по сетям общего пользования или по беспроводным сетям, а также для защиты подключенных систем и приложений. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 9.10 | *Контроль* | **Мобильные устройства, работа из дома или удаленная работа и съемные носители** |
| | *Описание* | В организации есть соответствующие механизмы для управления рисками безопасности при использовании мобильных устройств, работы из дома или удаленной работы и съемных носителей. |
| | *Ожидания* | • В организации есть политики и процедуры для мобильных устройств и работы из дома/удаленной работы, которые демонстрируют подход организации к управлению соответствующими рисками безопасности.<br>• В организации есть средства защиты, позволяющие избежать несанкционированного доступа или раскрытия информации, обрабатываемой мобильными устройствами, например, возможности шифрования и удаленного уничтожения данных.<br>• Организация применяет меры безопасности для защиты информации, обрабатываемой при работе из дома или удаленной работе, например VPN и двухфакторную аутентификацию.<br>• Если есть бизнес-необходимость хранить ПД на съемных носителях, организация минимизирует объем хранимых таким образом ПД, а также внедряет программное решение для установления разрешений или ограничений в отношении отдельных устройств или целого класса устройств.<br>• Организация использует самую современную версию выбранного решения для удаленного доступа. Организация можете поддерживать и обновлять устройства удаленно.<br>• Организация не разрешает выносить оборудование, информацию или программное обеспечение за пределы своей территории без предварительного разрешения. В организации есть журнал учета всех используемых мобильных устройств и съемных носителей с указанием лиц, которым они выделены. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Recommendations to protect personal data in situations of mobility and telecommuting (Agencia Española de Protección de Datos, April 2020)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 9.11 | *Контроль* | **Защищенные зоны** |
| | *Описание* | Организация защищает свои физические офисы, чтобы предотвратить несанкционированный доступ или повреждение ПД, а также вмешательство в обработку ПД. |

| | | |
|---|---|---|
| | *Ожидания* | • Организация обеспечивает защиту определенных зоны (зоны, содержащие конфиденциальную или важную информацию) с помощью соответствующих средств контроля доступа, таких как двери и замки, сигнализация, охранное освещение или видеонаблюдение.<br>• В организации есть порядок приёма посетителей, такие как процедуры регистрации, именные бейджи и доступ в сопровождении сотрудника.<br>• Организация реализует дополнительную защиту от внешних и экологических угроз в защищенных зонах, таких как серверные помещения.<br>• Офисное оборудование размещено и защищено надлежащим образом, чтобы снизить риски, связанные с экологическими угрозами и возможностями несанкционированного доступа.<br>• Организация хранит бумажные документы в надежном месте и контролирует доступ к ним.<br>• В организации действует политика «чистого стола» (Clear Desk Policy) и иные правила защиты данных в отношении рабочих мест, где обрабатываются ПД.<br>• Организация регулярно проводит проверку соблюдения правил защиты данных на рабочих местах и надлежащим образом устраняет выявляемые проблемы.<br>• Организация применяет политику «чистого экрана» (Clear Screen Policy) в отношении рабочих мест, где обрабатываются ПД. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018)<br>• Opinion 2/2017 on data processing at work, WP249 |
| 9.12 | *Контроль* | **Непрерывность бизнес-процессов, восстановление после аварий и резервное копирование** |
| | *Описание* | В организации есть планы по устранению серьезных сбоев, и организация создает резервные копии ключевых систем, приложений и данных для предотвращения потери ПД. |
| | *Ожидания* | • В организации есть основанный на рисках План обеспечения непрерывности бизнес-процессов (BCP) для устранения сбоев и План аварийного восстановления (DRP) для устранения последствий стихийных бедствий, в которых определяются записи, имеющие решающее значение для дальнейшего функционирования организации.<br>• Организация создает резервные копии электронной информации, программного обеспечения и систем (и, в идеале, хранит их за пределами своей территории).<br>• Частота резервного копирования отражает чувствительность и важность данных.<br>• Организация регулярно тестирует резервные копии и процессы восстановления, чтобы убедиться, что они соответствуют своему назначению. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |

## 10. Реагирование на нарушения и мониторинг

Организация должна уметь обнаруживать, расследовать, оценивать риски для защиты данных и регистрировать любые нарушения[3]. Организация должна сообщать о них соответствующим образом. Наличие эффективных процессов поможет организации в этом. Нарушение безопасности ПД может иметь целый ряд неблагоприятных последствий для субъектов данных. Это также может иметь серьезные последствия для организации, её персонала и клиентов, такие как финансовые санкции, ущерб для репутации, потеря бизнеса и применение дисциплинарных мер.

| | | |
|---|---|---|
| 10.1 | *Контроль* | **Обнаружение, управление и регистрация инцидентов и нарушений** |
| | *Описание* | В организации есть процедуры, обеспечивающие обнаружение, управление и надлежащую регистрацию инцидентов ИБ и нарушений безопасности ПД. |
| | *Ожидания* | • Организация проводит соответствующее обучение, чтобы персонал мог распознать инцидент ИБ и нарушение безопасности ПД.<br>• Уполномоченное лицо или группа управляет инцидентами ИБ и нарушениями безопасности ПД.<br>• Персонал знает, как быстро сообщить об инциденте или нарушении соответствующему лицу или группе для установления действительности такого события.<br>• Процедуры и системы облегчают ведение учета инцидентов и нарушений.<br>• У организации есть план для оперативного реагирования на любые возникающие инциденты ИБ и нарушения безопасности ПД.<br>• Организация централизованно регистрирует/записывает/документирует как фактические нарушения, так и потенциально опасные ситуации (даже если о них не нужно сообщать SA или субъектам данных).<br>• Документируются (например, в специальном журнале) факты, касающиеся потенциально опасных ситуаций или нарушений, в том числе:<br>- причины события;<br>- описание события;<br>- затронутые ПД;<br>- последствия инцидента или нарушения;<br>- любые принятые меры по исправлению положения и их обоснование. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Personal Data Breach Notification (Agencia Española de Protección de Datos, May 2021)<br>• Guidelines on Personal data breaches (Information Commissioner's Office, January 2021)<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• A Practical Guide to Personal Data Breach Notifications under the GDPR (Data Protection Commission, October 2019)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 10.2 | *Контроль* | **Оценка и сообщение о нарушениях** |
| | *Описание* | В организации есть процедуры для оценки всех инцидентов ИБ и нарушений безопасности ПД, а также для сообщения о них в SA в установленные сроки. |

[3] Здесь и далее под «нарушением» понимается нарушение безопасности ПД.

| | | |
|---|---|---|
| | *Ожидания* | • В организации есть процедура для оценки вероятности и серьезности риска для субъектов данных в результате нарушения безопасности ПД.<br>• В организации есть процедура сообщения в SA о нарушении в течение 72 часов с момента получения информации об этом (даже если полная информация еще недоступна), и организация своевременно информирует SA.<br>• Процедура включает в себя подробную информацию о том, какие данные о нарушении должны быть предоставлены SA.<br>• Если организация считает ненужным сообщать о нарушении, она документирует свои аугменты в пользу того, что нарушение вряд ли приведет к риску для прав и свобод субъектов данных. |
| | *Ссылки* | • GDPR: ст.33; rc.75, 85, 87-88<br>• EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification<br>• Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01<br>• Opinion 03/2014 on Personal Data Breach Notification, WP213<br>• Guidelines on Personal Data Breach Notification (Agencia Española de Protección de Datos, May 2021)<br>• Guidelines on Personal data breaches (Information Commissioner's Office, January 2021)<br>• A Practical Guide to Personal Data Breach Notifications under the GDPR (Data Protection Commission, October 2019) |
| 10.3 | *Контроль* | **Уведомление субъектов данных** |
| | *Описание* | В организации есть процедуры для уведомления субъектов данных, пострадавших от нарушения безопасности их ПД, если такое нарушение может привести к высокому риску для прав и свобод субъектов. |
| | *Ожидания* | • В организации есть процедура, определяющая порядок сообщения пострадавшим субъектам данных о нарушении, если оно может привести к высокому риску для их прав и свобод.<br>• Организация сообщает субъектам данных о нарушениях безопасности ПД ясным, понятным языком без неоправданной задержки.<br>• Информация, которую организация предоставляет субъектам данных, включает в себя контактные данные DPO, описание вероятных последствий нарушения и принятых мер (включая действия по уменьшению вреда и любые возможные неблагоприятные последствия).<br>• Организация предоставляет субъектам данных рекомендации по защите от любых последствий нарушения безопасности их данных. |
| | *Ссылки* | • GDPR: ст.34; rc.75, 86-88<br>• EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification<br>• Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01<br>• Opinion 03/2014 on Personal Data Breach Notification, WP213<br>• Guidelines on Personal Data Breach Notification (Agencia Española de Protección de Datos, May 2021)<br>• Guidelines on Personal data breaches (Information Commissioner's Office, January 2021)<br>• A Practical Guide to Personal Data Breach Notifications under the GDPR (Data Protection Commission, October 2019) |
| 10.4 | *Контроль* | **Обзор и мониторинг нарушений** |
| | *Описание* | Организация осуществляет обзор и мониторинг нарушений безопасности ПД |
| | *Ожидания* | • Организация анализирует все сообщения о нарушениях безопасности ПД, чтобы предотвратить их повторение.<br>• Организация отслеживает тип, объем и стоимость нарушений.<br>• Организация проводит анализ тенденций в отчетах о нарушениях за определенный период времени, чтобы понять их причины и существо.<br>• Группы, отвечающие за управление и практическую реализацию защиты данных, проверяют результаты вышеупомянутого анализа. |
| | *Ссылки* | • GDPR: ст.32; rc.74-77, 83<br>• Guidelines on Personal Data Breach Notification (Agencia Española de Protección de Datos, May 2021)<br>• Guidelines on Personal data breaches (Information Commissioner's Office, January 2021)<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guidance for Controllers on Data Security (Data Protection Commission, February 2020)<br>• A Practical Guide to Personal Data Breach Notifications under the GDPR (Data Protection Commission, October 2019)<br>• Guidelines on Security of Personal Data (Commission Nationale de l'Informatique et des Libertés, 2018) |
| 10.5 | *Контроль* | **Внешний аудит или проверка соответствия** |
| | *Описание* | Организация проводит внешний аудит управления и практической реализации защиты данных или другую процедуру проверки соответствия. |
| | *Ожидания* | • Организация использует предоставленные внешними организациями инструменты самостоятельной оценки для обеспечения гарантий соответствия требованиям по защите данных и ИБ.<br>• Организация подпадает под проведение внешнего аудита или пользуется услугами внешнего аудитора для предоставления независимых гарантий (или сертификации) соответствия требованиям по защите данных и ИБ.<br>• Организация придерживается соответствующего кодекса поведения или практики для своего сектора (если таковой существует).<br>• Организация составляет аудиторские отчеты для документирования полученных результатов.<br>• В организации есть централизованный план действий по внедрению результатов аудита по управлению и практической реализацией защиты данных. |
| | *Ссылки* | • GDPR: ст.40, 42; rc.98-100<br>• EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679<br>• EDPB, Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation |
| 10.6 | *Контроль* | **Программа внутреннего аудита** |
| | *Описание* | Если в организации есть программа внутреннего аудита, она достаточно подробно охватывает управление и практическую реализацию защиты данных (например, безопасность и управление записями). |
| | *Ожидания* | • Организация контролирует соблюдение требований по защите данных и регулярно проверяет эффективность применяемых мер.<br>• Организация регулярно проверяет соблюдение персоналом политик и процедур управления и практической реализации защиты данных.<br>• Организация регулярно проводит неформальный специальный мониторинг и выборочные проверки.<br>• Организация обеспечивает беспристрастный мониторинг соблюдения политик и процедур – безотносительно реализующих их лиц. |

| | | |
|---|---|---|
| | | • В организации есть централизованный план-график аудита, чтобы продемонстрировать планирование внутренних аудитов защиты данных.<br>• Организация составляет аудиторские отчеты для документирования полученных результатов.<br>• В организации есть централизованный план действий по анализу и использованию результатов аудита защиты данных. |
| | *Ссылки* | • GDPR: ст.39<br>• Guidelines on Data Protection Officers ('DPO'), WP243 rev.01<br>• Guidelines pratique RGPD - Délégués à la protection des données (Commission Nationale de l'Informatique et des Libertés, Novembre 2021) |
| 10.7 | *Контроль* | **Информация об эффективности и соответствии требованиям** |
| | *Описание* | У организации есть бизнес-цели, связанные с соблюдением требований к защите данных, и организация может получить доступ к соответствующей информации для оценки степени соблюдения таких требований. |
| | *Ожидания* | • В организации есть KPI, касающиеся выполнения запросов субъектов на доступ к их данным (DSAR) (количество запросов и процент выполнения в установленные сроки).<br>• В организации есть KPI, касающиеся обучения управлению практической реализации защиты данных, включая отчет с указанием на долю прошедшего такое обучение персонала.<br>• В организации есть KPI, касающиеся ИБ, включая количество нарушений безопасности ПД, инцидентов ИБ и потенциально опасных ситуаций.<br>• В организации есть KPI, касающиеся управления записями, включая использование таких показателей, как статистика выполнения поиска записей, соблюдение сроков удаления и эффективность существующей системы для индексирования и отслеживания бумажных документов с ПД. |
| | *Ссылки* | • GDPR: ст.24-25, 32; rc.74-78, 83<br>• EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default<br>• EDPS Opinion 5/2018 Preliminary Opinion on privacy by design<br>• Guidelines on Data Security (Information Commissioner's Office, January 2021)<br>• Guía de Protección de Datos por Defecto (Agencia Española de Protección de Datos, Octobre 2020)<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |
| 10.8 | *Контроль* | **Использование управленческой информации** |
| | *Описание* | Вся соответствующая управленческая информация и результаты деятельности по мониторингу и обзору доводятся до сведения соответствующих внутренних сторон, включая, при необходимости, руководство организации. Эта информация служит основой для обсуждений и дальнейших действий в области защиты данных. |
| | *Ожидания* | • В организации есть панель мониторинга защиты данных (privacy dashboard), дающая общую картину всех ключевых показателей эффективности управления и практической реализации защиты данных.<br>• Группа (группы), осуществляющие надзор за управлением и практической реализацией защиты данных, регулярно обсуждают KPI, а также результаты мониторинга и обзоров.<br>• KPI управления и практической реализации защиты данных, а также результаты мониторинга и обзоров регулярно обсуждаются группами на оперативном уровне. |
| | *Ссылки* | • GDPR: ст.24; rc.74-77, 83<br>• Guidelines on the Accountability Framework to demonstrate data protection compliance (Information Commissioner's Office, September 2020) |

**Документированная информация, позволяющая объективно продемонстрировать соблюдение требований GDPR**

1. Guideline for data inventory and processing activities mapping
2. Data retention policy and schedule
3. Data deletion register
4. Analytical reports on data inventory and processing
5. RoPA maintenance guideline
6. RoPA for data controller
7. RoPA for data processor (if applicable)
8. Privacy policy
9. Lawful basis selection reports
10. Data subject consent obtaining guideline
11. Customer consent and withdrawal forms
12. Clauses for customer agreements
13. Paternal consent and withdrawal forms
14. Staff consent and withdrawal forms
15. Clauses for staff agreements
16. LIA performance and review guideline
17. LIA outcomes (reports)
18. LIA reports register
19. Report on absence of necessity to designate a representative in the EEA
20. Privacy policy (including annex with DPDD methodology)
21. Information security policy
22. Plan for reviewing policies and procedures
23. Staff briefing log concerning policies and procedures
24. Awareness plan, handouts and posters
25. Staff training policy (programme)
26. Staff training log
27. Training materials
28. Data subject request handling guideline
29. Data subject request forms
30. Response forms to data subject request
31. Data subject request and response register

32. Response performance and quality reports
33. Privacy notification guideline
34. Privacy notice for data subjects
35. Online privacy notice
36. Register of privacy notices
37. Cookie's preference dashboards
38. Employee privacy notice
39. Data sharing guideline
40. Data transfer/processing/management agreement forms
41. Counterparties compliance questionnaires
42. Counterparties audit reports
43. International (from EEA to non-EEA) data transfer guideline
44. TIA performance and review guideline
45. TIA outcomes (reports)
46. TIA reports register
47. Privacy policy (including annex with DPIA methodology)
48. DPIA performance and review guideline
49. DPIA outcomes (reports)
50. DPIA reports register
51. Report on absence of necessity of DPIA performance
52. Information security policy and change register
53. Staff acceptable use policy
54. Encryption policy
55. Bring your own device policy
56. Clear desk and clear screen policy
57. Mobile device and teleworker policy
58. Password policy construction policy
59. Pseudonymization and anonymization guideline
60. Business continuity plan
61. Disaster recovery plan
62. Data breach handling guideline and action plans
63. Data breach register
64. Data breach notification and communication forms
65. Data breach analysis reports
66. Internal audit policy and programme
67. Internal audit checklist
68. Internal audit reports and action plans

**Перечень сокращений и их расшифровки**

| Сокращение | Расшифровка |
|---|---|
| Государство-член | Государство, являющееся действующим участником ЕЕА |
| ЕС | Европейский Союз |
| ИБ | Информационная безопасность |
| ПД или данные | Персональные данные |
| BCR | Binding Corporate Rules (Обязательные корпоративные правила) |
| DPA | Data Processing Agreement (Соглашение об обработке ПД) |
| DPIA | Data Protection Impact Assessment (Оценка воздействия на защиту ПД) |
| DPO | Data Protection Officer (Инспектор по защите ПД) |
| GDPR | General Data Protection Regulation (Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС) |
| EDPB | European Data Protection Board (Европейский совет по защите данных) |
| EDPS | European Data Protection Supervisor (Европейский инспектор по защите данных) |
| EEA | European Economic Area (Европейская экономическая зона)[4] |
| KPI | Key Performance Indicator (Ключевой показатель эффективности) |
| LIA | Legitimate Interest Assessment (Оценка возможности использовать законный интерес как правового основания обработки ПД) |
| DPDD | Data Protection by Design and by Default (Защита ПД: проектируемая и по умолчанию) |
| rc. | Обозначение номера пункта (Recital) из преамбулы к GDPR |
| RoPA | Records of Processing Activities (Реестр деятельности по обработке ПД) |
| SA | Supervisory Authority (Надзорный орган) в ЕЕА |
| SCC | Standard Contractual Clauses (Стандартные договорные условия, принятые Европейской Комиссией) |
| TIA | Transfer Impact Assessment (Оценка трансграничной передачи ПД) |
| WP29 | Data Protection Working Party 29 (Рабочая группа по защите физических лиц при обработке ПД – предшественник EDPB) |

[4] Для целей настоящего документа используется для обозначения стран, в которых применяются нормы GDPR – государства-члены Европейского Союза и некоторые государства-члены Европейской ассоциации свободной торговли (Норвегия, Исландия и Лихтенштейн). По состоянию на 30.11.2021г. Великобритания и Швейцария формально не являются государствами-членами ЕЕА, и в указанных странах нормы GDPR прямо не применяются, хотя национальное законодательство этих стран о ПД в максимальной степени гармонизировано с положениями GDPR.