IT-право Защита данных ПРАВО

Каталог обработки [Требования по обработке, согласно Регламенту защиты данных ЕС, DS-GVO/GDPR]

Posted on 10.07.202010.07.2020 Author Roman Pusep

Практические советы и нормативное содержание учета процессов по требованиям Регламента защиты данных (DS-GVO/GDPR)

В соответствии со статьей 30 Общего регламента защиты данных ЕС (DS-GVO), большинству предприятий необходимо вести учет операций по обработке персональных данных (каталог обработки / реестр операций обработки (Verzeichnis von Verarbeitungstätigkeiten).

Тем не менее, создать и вести каталог обработки не так просто. У должностных лиц ответственных за защиту данных и у руководства компаний, даже спустя 2 года действия DS-GVO, нет ясности в том, как организовать защиту данных в целом, и в частности регистрировать процессы обработки, какую информацию следует вносить в каталог и как правильно его вести.

В данной публикации, адвокаты в сфере IT-права Роман Пусеп и Кристина Димитрова объясняют нормативное содержание и требования законодательства о защите данных по документированию обработки данных, а также дают советы по ведению этого каталога.

Обязанность вести учетные сведения об обработке

С 25 мая 2018 года введена обязанность вести новый каталог регистрации действий по обработке, что предусмотрено статьей 30 (DS-GVO). Ранее, подобный реестр требовалось вести в соответствии с Федеральным законом о защите данных (BDSG). Принципиальное отличие от старого списка процедур, предусмотренных §§ 2, 2g и 4g BDSG, состоит в том, что новый список не является открытым для общественности, согласно статье 30 пункта 4 DS-GVO. Только орган надзора имеет право запрашивать новый каталог.

Содержание и правовые последствия статьи 30 DS-GVO

Согласно статье 30 DS-GVO, список действий по обработке, подтверждает, что данные обрабатываются в соответствии с требованиями DS-GVO. В то же время, ответственные лица выполняют, ведя список действий по обработке персональных данных, свои обязанности на основании ст. 5 п. 2 DS-GVO.

Кто обязан регистрировать действия и вести каталог обработки

Обязанность составлять и вести список процессов обработки возлагается на:

- контролера, т.е. ответственное лицо (ст. 30 п. 1 DS-GVO);
- обработчиков, т.е. процессоров (ст. 30 п. 2 DS-GVO);
- ЕС-представителей контролеров и процессоров (ст. 27 DS-GVO, ст. 30 п. 2 DS-GVO).

Когда нужно вести каталог обработки

Исключение: Согласно статье 30 п. 5 DS-GVO, операции по обработке не нужно документировать, если в компании работает менее 250 сотрудников.

В этом же параграфе (статье) предусмотрено три встречных исключения. Ими устанавливается обязательное ведение каталога обработки, если контроллер или процессор обрабатывает персональные данные, которые

- представляют риск для прав и свобод субъектов данных (например, видеонаблюдение, процесс оценки кредитоспособности, местонахождение сотрудников), или
- специальные категории данных в соответствии со ст. 9 п. 1 DS-GVO (например, религиозная принадлежность, информация о здоровье, биометрические данные) или уголовные судимости и преступления в значении ст. 10 DS-GVO или
- обработка осуществляет не только время от времени (например, обработка данных о клиентах или сотрудниках, ведение учетных записей электронной почты).

В связи с тремя вышеупомянутыми группами, исключение из обязательства по ст. 30 DS-GVO очень редкое, и многим ответственным лицам, с численностью персонала менее 250 человек, придется создавать и вести каталог.

Содержание каталога

Информация, которую ответственные лица и обработчики должны регистрировать при создании и ведении каталога, различна от ответственного субъекта (см. ниже).

Следует подчеркнуть, что список обязанностей процессора значительно короче, чем у ответственного лица, поскольку процессор связан инструкциями.

Что такое «обработка данных»

Термин «обработка данных» в соответствии со ст. 4 п. 2 DS-GVO является очень широким и охватывает процесс или серию процессов со ссылкой на персональные личные данные, такие как сбор, запись, организация, хранение, изменения, запрос, использование, передача.

Приведем несколько примеров из корпоративной практики: это все процессы, связанные с регистрацией времени, основными данными клиентов, расчетом заработной платы, рассылкой новостей, прочее.

Обязанности ответственного лица согласно ст. 30 ч. 1 п. 2 DS-GVO

В Каталоге должна быть зафиксирована, по крайней мере, следующая информация:

- имя и контактные данные ответственного лица, а также лица, которое может нести совместную ответственность с ним, представителя и сотрудника (должностного лица) по защите данных;
- цели обработки;
- описание категорий субъектов данных и персональных данных;
- категории получателей, которым были или будут раскрыты данные, включая получателей в третьих странах или международных организациях;
- передача личных данных третьей стране или международной организации; запланированные периоды удаления различных категорий данных;
- общее описание технических и организационных мер в соответствии со ст. 32 DS-GVO.

Документирование цели каждого вида обработки обязано быть четким и понятным. Это делается для того, чтобы каждое ответственное лицо перед обработкой личных данных продумало о том, для чего именно ему нужны эти данные.

В идеале это означает, что обрабатываются только те данные, которые требуются и только в той мере, которая требуется для достижения конкретной цели.

Получатель данных также может быть частью своей или материнской компании контролера (ответственного лица), банков, налоговых органов и других потенциальных получателей персональных данных.

В случае передачи данных в третью страну или в международную организацию, следует отметить, что ответственное лицо обязано документально подтвердить свою оценку и соответствующие гарантии в соответствии со ст. 49 п. 6 DS-GVO.

Обязанности обработчика согласно ст. 30 п. 2 Регламента защиты данных (DS-GVO)

Из вышеупомянутых обязанностей ответственного лица, обязательства в соответствии со ст. 30 п. 2 лит. c), d) и f) DS-GVO не имеет отношения к процессору. Он должен заявить следующее:

- имя и контактные данные процессора и каждого контроллера, от имени которого работает процессор, представителя контроллера или процессора и сотрудника по защите данных;
- категории обработки, выполняемые от имени каждого ответственного лица; передача персональных данных в третью страну или в международную организацию;
- общее описание технических и организационных мер в соответствии со статьей 32 DS-GVO.

Тут особенно важно подчеркнуть, что процессор обрабатывает свой собственный каталог, а не просто ссылается на каталог ответственного лица (контроллера).

Обязанностью обработчика, которая косвенно вытекает из ст. 28 п. 3 лит. a) DS-GVO, является документирование инструкций лица, ответственного за обработку данных.

Форма Каталога

Согласно ст. 30 DS-GVO списки должны храниться в письменном виде. Но, согласно ст. 30 п. 3 DS-GVO, допускается ведение Каталога в электронном формате, с помощью специального программного обеспечения для защиты данных.

В частности, процессоры, которые предлагают стандартизированные продукты или услуги (например, облачные вычисления, центры обработки вызовов), имеют возможность группировать обработку на том же уровне, которая была введена в эксплуатацию, и назначать ответственных за эти группы. Таким образом, например, в смысле регулирования можно вводить информацию о целях обработки очень эффективно и практически в табличной форме. Процессор может вести общий / генеральный каталог обработки данных, не ведя такой каталог для каждого ответственного лица.

Как часто следует обновлять и вносить данные в каталог обработки?

Регламент защиты данных явно не указывает на обязательство обновление каталога. Такое обязательство может быть выведено из подотчетности в соответствии со статьей 5 пункта 2 DS-GVO. Ответственное лицо обязано не только соблюдать принципы защиты данных, но и быть в состоянии продемонстрировать их соответствие.

Регламент не устанавливает предельный срок для предоставления учетной записи. Исходя из этого, можно сделать вывод, что ответственное лицо должно быть в состоянии сделать это в любое время. Поэтому каждое ответственное лицо и каждый обработчик (процессор) должны постоянно обновлять свой собственный каталог.

Ответственность за нарушения ст. 30 DS-GVO

Согласно ст. 83 п. 4 лит. a) DS-GVO, следующие нарушения приводят к штрафу до 10 миллионов евро или до 2 % от годового оборота компании:

- каталог отсутствует;
- неполное ведение каталога;
- отказ от сотрудничества с органом надзора, в т.ч. не предоставление Каталога обработки.

Следует отметить, что раньше, на практике, органы надзора по-разному определяли наказание за нарушение положений Регламента защиты данных. Поэтому летом 2019 года была принята новая Концепция DSK для точного расчета денежных штрафов за несоблюдение защиты данных. Согласно DSK, размеры штрафов теперь варьируются в зависимости от оборота и класса компаний. Но даже для микропредприятий, отсутствие каталога может повлечь наложение штрафных санкций в несколько тысяч евро.

Язык каталога обработки

Согласно немецкому административно-процессуальному законодательству (VwGO) официальным языком ведения документации в Германии является немецкий язык. Исходя из этого, Каталог рекомендуется вести на немецком языке. Международные компании с иным корпоративным языком, могут вести Каталог на другом языке, например на английском. Но, в таком случае, если немецкий контролирующий орган будет запрашивать доступ к документации по защите данных, вероятнее всего, компании придется предоставлять переводы всех запрашиваемых документов.

Требования к иностранным предприятиям

Часто иностранные компании не имеют своих представительств на территории ЕС, но, при этом, взаимодействуют с гражданами Евросоюза (собирают и обрабатывают персональные данные субъектов персональных данных ЕС). В таких случаях, иностранные фирмы (например из США, Российской федерации, Украины и др. стран) обязаны выполнять требования DS-GVO, в частности указать / назначить представителя в ЕС в соответствии со ст. 27 DS-GVO.

Это может происходить в случаях:

- выполнения части бизнес-процессов (работ) для европейских компаний, которые включают обработку и дальнейшую трансграничную передачу персональных данных;
- продажи товаров или услуг европейским субъектам персональных данных; осуществления мониторинга за действиями граждан ЕС;
- прочих действий, которые подразумевают сбор и обработку данных субъектов персональных данных.

Таким образом, иностранный бизнес должен не только выполнять требования по защите данных, а и продемонстрировать контролирующим органам их реализацию, в том числе ведение каталога обработки.

Выводы

WERNER Rechtsanwälte Informatiker рекомендует изучить законодательство и ответственно подойти к реализации его требований.

1. Изначально следует проверить обязанность ведения и создания каталога обработки.
2. Далее, нужно определить, в каких случаях персональные данные, например, от клиентов, поставщиков или сотрудников, собираются и обрабатываются.
3. С этой целью имеет смысл проведение соответствующего аудита.
4. Информация о процессах должна быть индивидуально адаптирована к бизнесу компании.
5. Не следует копировать чужой каталог. Для каждого процесса обработки нужно будет вести свой каталог (например, система финансового учета, система CRM, учет заработной платы).

Обзор некоторых типичных обработок:

- управление контактами;
- персонал (HR);
- учет заработной платы;
- система CRM;
- электронная почта;
- финансовый учет;
- назначение управления;
- администрация;
- взыскание долгов;
- веб-сайт;
- маркетинг;
- производство
- управление проектом;
- информация о покупателях;
- база самозанятых лиц (фрилансеров);
- видеонаблюдение;
- время хранения записи.

Шаблоны (образцы) Каталога обработки

В интернете доступны шаблоны таблиц для ведения Каталога обработки. Для удобства приведем ссылки для скачивания образцов Каталога обработки с сайта ldi.nrw.de (в PDF):

Образец Каталога обработки для ответственных лиц (Muster für Verantwortliche, VA)

Образец Каталога обработки для процессоров, обработчиков (Muster für Auftragsverarbeiter, AV)

Адвокаты WERNER Rechtsanwälte Informatiker будут рады поддержать вас по всем вопросам, связанным с организацией защиты данных.

https://www.werner-ri.de

Автор русской версии: RA Roman Pusep