Oļegs Sedjakins, mg. iur., doktorants
Baltijas Starptautiskā akadēmija
Latvija

Regula 2016/679: Tiesību uz personas datu pārnesamību ieviešana

Anotācija. ES Vispārīgā datu aizsardzības regula, jeb Regula 2016/679 (VDAR), pieņemta 2016.gada aprīlī, stājas spēkā 2018.gada 25.maijā. Būtiskas izmaiņas datu aizsardzības procesā notiks pēc Regulas stāšanas spēkā, tamdēļ pēdējo mēnešu laikā ir krasi pieaugusi privātā sektora paaugstināta interese par personas datu aizsardzības nodrošināšanas aspektiem. VDAR ievieš personas datu aizsardzības terminoloģijā jaunās tiesības – tiesību uz datu apriti, kā arī tiesību uz datu dzēšanu (tiesība „tikt aizmirstam") . Autors izklāsta personas datu aprites tiesības būtību, raksturo tās saistību ar pārējiem Regulas pantiem, kā arī pievērš uzmanību zināmām sarežģītībām, ar kurām privātajām biznesam, kas savā darbībā ievieš mehānismus, atbilstošus regulas prasībām, būs jāsaskaras.

Atslēgas vārdi: Eiropas Savienība (ES), personas dati, datu aprite, Regula 2016/679.

Олег Седякин, mg. iur., докторант
Балтийская Международная Академия
Латвия

Регламент 2016/679: Учреждение права на переносимость личных данных

Аннотация. Регламент Европейского Союза 2016/679, принятый в апреле 2016 года, вступает в силу 25 мая этого года. Со вступлением в силу упомянутого Регламента в сфере обеспечения защиты личных данных произойдут значительные изменения, и в связи с этим, в последние месяцы резко возрос интерес частного сектора к аспектам обеспечения защиты личных данных. Регламент вводит в терминологию защиты личных данных новое право – право на переносимость данных, наряду с правом на забвение. Автор статьи раскрывает сущность права на переносимость данных, характеризует его связь с другими статьями Регламента, а также обращает внимание на основные сложности, с которыми придётся столкнуться частному сектору, внедряющему в свою деятельность механизмы, соответствующие требованиям Регламента.

Ключевые слова: Европейский Союз (ЕС), личные данные, переносимость данных, Регламент 2016/679

Oleg Sedyakin, mg. iur., doctoral student
Baltic International Academy
Latvia

Regulation 2016/679: Introduction of the right to data portability

Abstract. EU General Data Protection Regulation, or Regulation 2016/679 (GDPR), adopted in April 2016, comes in force in 2018, 25th May. Significant changes in data protection procedure are going to happen after the date and because of that, we can observe right now an increased attention of a private sector to methods and practices of data protection. GDPR introduces the new right into data protection legislation – the right to data portability, along with the right to erasure (or right "to be forgotten"). The author describes the essence of the introduced right to data portability, distinguishes its relations with regards to other provisions of the Regulation and draws attention to the main challenges, which will be faced by private business in the GDPR implementation process.

Keywords: European Union (EU), personal data, data portability, Regulation 2016/679

Введение: предпосылки появления Регламента 2016/679

Обработка личных данных, в ретроспективе, является сравнительно новой категорией, подпадающей под нормы правового регулирования, несмотря на то, что обработка информации, в широком понимании этого термина, происходила давно. Например, информация, получаемая тайными агентами о лицах, представляющих интерес организаторам сбора информации. Полученная таким образом информация могла быть использована в разных целях, от личных интересов монархов, до войны или дипломатии.

В настоящее время сбор и обработка личной информации предоставляют возможность лицам, осуществляющим подобные операции, составлять определённый «портфель» информации о практически любом лице: например, о его увлечениях, о его интересах, или даже о предполагаемых реакциях на события. Такая информация представляет не только бихевиористический и психоаналитический интерес, но и непосредственный интерес экономического характера. С постепенным приобретением информацией экономической значимости, появилась необходимость правового регулирования новой категории современной экономики – информации и данных.

Защита личных данных приобрела широкое распространение в правовом регулировании конца XX века. Для современной юрисдикции Европейского Союза (ЕС) основным нормативно-правовым актом, который сближал среди юрисдикций стран-участниц ЕС основы защиты личных данных, чем обеспечивал защиту фундаментальных прав и свобод, а также закреплял существование свободного потока данных внутри ЕС [1, Recital 3], являлась Директива 95/46/ЕС (далее - Директива), принятая ещё в 1995 году.

Директива, с целью защитить основные права и свободы физических лиц, в частности, права на приватность [1, ст. 1, п. 1], определила личные данные (*personal data*), как «любую информацию, относимую к идентифицированному или идентифицируемому физическому лицу (субъекту)», а также выделила базовые понятия, которые напрямую связаны с процессом обработки информации (обработка информации (*processing of personal data*), оператор (*processor*), получатель (*recipient*)) [1, ст. 2].

Несмотря на то, что Директива, внедрив в правовую систему различные понятия и принципы обработки личных данных, позволила странам-участницам усовершенствовать (а в некоторых случаях – поспособствовала появлению правового регулирования) национальное нормативно-правовое регулирование по вопросу защиты данных физических лиц, она уже не могла отвечать современной действительности и не предотвращала фрагментарную имплементацию или толкование принципов защиты личных данных физических лиц [2, Recital 9].

На основании этого, в рамках проекта Единого Европейского Цифрового Рынка (*European Digital Single Market*) [3, п. 45], был принят Регламент об общей защите данных (*General Data Protection Regulation;* необходимо принимать во внимание, что в некоторых источниках на русском языке, его называют Генеральным Регламентом о защите данных). Таким образом, первым значимым изменением стала смена характера нормативно-правового акта с Директивы на Регламент, что, в свою очередь, означает приобретение моделью правового регулирования, закреплённой в Регламенте, в отношении защиты данных физических лиц, обязательного, всецелого и прямого характера действия для всех стран-участниц ЕС [4, ст. 288].

Регламент 2016/679: основные нововведения

Несмотря на введение нового нормативно-правового регулирования, Регламент сохраняет центральное понятие личных данных в точности, каким оно было представлено в Директиве [1, ст. 2, п. a; 2, ст. 4, п. 1].

Однако Регламентом расширяется понятийный аппарат, посредством внедрения новых терминов, таких как: «профилирование» (*profiling*), «псевдонимизация» (*pseudonymisation*), «генетические данные» (*genetic data*), «биометрические данные» (*biometric data*), «трансграничная обработка» (*cross-border processing*) и другие термины [3, ст. 4].

Помимо расширения понятийного аппарата, к принципам обработки данных, также был присоединён новый принцип – обеспечение сохранности личных данных [2, ст. 5, п. 1f], означающий принятие достаточных и необходимых технических или организаторских мер, которые могут воспрепятствовать незаконному или неправомочному доступу к информации и её обработке.

Существенное развитие получила категория согласия субъекта на обработку личных данных. Если в Директиве согласие субъекта упоминалось, как одно из условий для обеспечения законности обработки личных данных [1, ст. 7, п. a], в том числе и особой категории личных данных – сенситивных данных [1, ст. 8, ч. 2, п. a], то в Регламенте согласию субъекта данных посвящены уже несколько отдельных статей, в которых дополнительно урегулированы: базовые условия для обеспечения действительности согласия [2, ст. 7] и условия, требуемые к соблюдению, в отношении согласия ребёнка на пользование услугами информационного сообщества [2, ст. 8].

Понятие особой категории личных данных (*сенситивных данных*) было расширено с принятием Регламента. Если Директивой к особой категории относили личные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, сведения об участии в профсоюзах, а также информацию о здоровье или сексуальной жизни лица [1, ч. 1, ст. 8]; то Регламент к сенситивным данным относит также генетические данные, биометрические данные и сведения о сексуальной ориентации физического лица [2, ч. 1, ст. 9].

Права субъекта данных, также приобрели более ярко выраженную структуру в тексте Регламента (по сравнению с Директивой): и были выделены в несколько категорий. В настоящей статье не предполагается рассмотрение всех категорий прав субъекта данных, а исключительно одного права, относимого к категории «прав субъекта на исправление и удаления личных данных», к которой относятся: право субъекта данных на исправление (*right to rectification*), право на удаление данных – «право на забвение» (*right to erasure ('right to be forgotten')*), право на запрет обработки данных (*right to restriction of processing*) и право на переносимость (портативность) данных (*right to data portability*).

Право на переносимость (портативность) данных

Помимо ранее упомянутых нововведений и изменений, Регламент вводит право субъекта на переносимость (портативность) данных (*right to data portability*) [2, ст. 20]. Это право в своей сущности обладает двумя основными составными элементами:

- Во-первых, этим правом закрепляется возможность субъекта данных **получить** касающиеся его или её и предоставленные контроллеру им лично данные, в структурированной и машиночитаемой форме; а также

- Право субъекта **передать** эти данные другому контроллеру без каких-либо препятствий со стороны контроллера, которому эти данные были предоставлены изначально [2, ст. 20, ч. 1, п. a, b].

Таким образом, прежде чем реализовывать право на портативность данных, необходимо удостовериться в наличии условий для осуществления такого права, а именно в том, что **данные**, подлежащие переносу, **должны быть предоставлены лично субъектом данных** и не получены контроллером из каких-либо других источников.

В связи с этим, контроллеру необходимо обращать особое внимание на “происхождение” данных, ведь, как Директива, так и в последствии Регламент, не сделали согласие исключительным основанием для обеспечения законности обработки личных данных - всего таких оснований шесть [1, ст. 7; 2, ст. 6, ч. 1]:

- Согласие субъекта данных на обработку его данных для одной или нескольких определённых целей;
- Обработка необходима для выполнения договорных обязательств, в которых одной из сторон является субъект данных, или, соответствнно, для вступления в договорные отношения (где необходимо выражение воли субъекта данных на вступление в такие отношения);
- Обработка необходима для выполнения обязательств, предписанных контроллеру законом;
- Обработка необходима для защиты жизненно важных интересов субъекта данных или другого физического лица;
- Обработка обусловлена возложенными на контроллера официальными полномочиями или обработка производится в общественных интересах;
- Обработка необходима для достижения законных интересов контроллера или третьих лиц, за исключением тех случаев, когда такие интересы пересекаются с фундаментальными правами и свободами субъекта данных, в особенности - детей.

При первом приближении, согласие полностью отвечает условию осуществления права на портативность данных (субъект данных должен лично предоставить свои данные), однако необходимо принимать во внимание и условия, которые Регламент предъявляет для обеспечения действительности согласия субъекта данных, в противном случае, возникает риск незаконной обработки информации, что впоследствии приводит к нарушению положений Регламента.

Рабочая группа по статье 29 (*Article 29 Working Party*), которая является консультативным органом, созданным под эгидой Директивы, предоставляет толкования в отношении различных аспектов защиты личных данных. В своём руководстве по праву на портативность данных (*Guidelines on the right to data portability*), приведён пример, при котором согласие может не быть действительным: “В отношении данных работников, право на портативность применяется только в случае, когда обработка обусловлена договором, в котором субъект данных - одна из сторон. В большинстве случаев, согласие не будет считаться свободно выраженным из-за отсутствия равноправия работодателя и работника.” [5, стр. 8].

Из этого следует, что правомерность обработки личных данных должна быть основана на пунктах a и b, ч. 1, ст. 6 Регламента. Или же, если переносу подлежат данные из особой категории (*сенситивные данные*), – основанием должна служить обработка личных данных в соответствии с п. a, ч. 2, ст. 9 Регламента; в дополнение к основаниям законности обработки личных данных,

необходимо принимать во внимание дополнительные требования, предъявляемые к согласию субъекта данных.

При дальнейшем анализе права на портативность данных, стоит обратить внимание на часть формулировки понятия права субъекта: "... личные данные, касающиеся его или её" [2, ст. 20, ч. 1]. При осуществлении лингвистического толкования понятия права на портативность данных в этой части, стоит заключить, что передача права на портативность данных не представляется возможной ни в какой форме, поскольку личные данные должны обладать признаком относимости к конкретному физическому лицу. И если такое физическое лицо, к которому относятся личные данные пытается передать право на портативность данных другому лицу, то контроллеру (или оператору, соответственно), при получении от доверенного лица заявления на перенос данных к другому контроллеру, следует отказывать в реализации права на портативность данных, поскольку это противоречит, как положению Регламента (право на портативность данных - это право субъекта данных), так и одному из принципов - принцип обработки, обеспечивающей достаточный уровень сохранности личных данных [2, ст. 5, ч. 1, п. f].

Причина такого ограничения со стороны законодателей лежит в развитии ярко выраженного и чётко определённого в Регламенте права на защиту личных данных [2, ст. 1, ч. 2] и его происхождения из понятия приватности, упомянутого в Директиве [1, ст. 1, ч. 1].

Второй структурный элемент, выраженный в праве субъекта на свободную передачу личных данных от одного контроллера другому тесно связан со всем упомянутым выше, а в особенности - с условиями, которые Регламент предписывает согласию субъекта данных.

Новый контроллер, к которому субъект "портирует" свои личные данные, не освобождается от соблюдения норм Регламента, то есть у него должна присутствовать законность обработки личных данных. Не составляет труда предположить, что основаниями обработки переданных личных данных будут либо согласие субъекта, либо договорные правоотношения.

Однако новому контроллеру также будет необходимо подтверждать наличие основания обработки личных данных и его соответствие всем условиям согласия (если законность обработки будет основана на согласии субъекта), а именно, контроллер должен суметь продемонстрировать, что субъект предоставил ему своё согласие на обработку личных данных [2, ст. 7, ч. 1] - из этого следует, что в случае возникновения спора, бремя доказывания по факту наличия согласия будет возложено на контроллера.

Критерии, предъявляемые Регламентом к доказательству согласия субъекта трактуются по-разному, но его техническая основа выражена в следующем требовании: "Если согласие субъекта данных дано в письменной декларации, которая затрагивает и иные вопросы, то согласие должно быть представлено в явно отличной от других вопросов, понятной и легкодоступной форме при ипользовани чёткого и ясного языка. Любая часть такой декларации, входящей в противоречие с настоящим Регламентом не будет считаться обязывающей" [2, ст. 7, ч. 2].

Такая формулировка, предписывающая существенное отличие выраженного субъектом согласия от других вопросов, вызывает некоторые споры, когда проецируется применение этого положения на практике. Если, при осуществлении доставки товара, у поставщика нет возможности не обрабатывать информацию о заказчике (поскольку, в противном случае он не сможет выполнить условия договора), то при оказании услуг професионального характера (бухгалтерские, юридические и другие) обработка декларированного адреса жительства не является настолько очевидно необходимой. В такой ситуации,

контроллеру необходимо получить согласие клиента на обработку его личных данных - но в какой форме? Достаточно ли пункта о согласии клиента на обработку его / её личных данных в договоре, или же необходимо выделять в договоре отдельный раздел, или же заключать отдельное соглашение приложением к договору?

Единого ответа на этот вопрос в настоящий момент нет, а потому, представляется, что ясность внесёт исключительно правоприменительная практика. К примеру, в рамках конференции “Digitālā Ēra 2017”, прошедшей в Риге 26 апреля 2017 года, представители Государственной Инспекции Данных (Datu Valsts Inspekcija, DVI), подчеркнули, что наилучшим вариантом они считают заключение отдельного соглашения, но были высказаны также и другие мнения.

Принимая во внимание значительный объём изменений, который затрагивает область защиты личных данных физических лиц, была предпринята возможность сократить процедуру переноса личных данных субъекта, не задействуя последнего в процессе переноса. В частности, в Регламенте отмечается, что при наличии технической возможности, процесс переноса данных от одного контроллера другому, может быть произведён напрямую, без посредничества субъекта данных [2, ст. 20, ч. 2].

Для предотвращения сложностей взаимодействия новых механизмов, представленных в Регламенте, был предпринят ряд ограничений на использование права на портативность данных. Как уже было проанализировано, использование права не будет происходить повсеместно, и помимо предписанных регламентом требований к использованию права (которые в некоторой форме ограничивают его применение), существуют также и прямо выраженный ограничения [2, ч. 3, 4, ст. 20], которые заключаются в следующем:

- Применение права на переносимость данных не должно препятствовать реализации права быть забытым;
- Применение права на переносимость данных невозможно, если обработка данных производится официальными учреждениями на законных основаниях и в общественных интересах; и
- Применение права на переносимость данных не должно затрагивать права и свободы других.

Заключение

Право на переносимость (портативность) данных является новой юридической конструкцией, внедрённой в рамки нормативно-правового регулирования о защите личных данных физических лиц. Эта конструкция обеспечивает достижение одной из целей Регламента - свободного потока данных в пределах Европейского Союза.

В связи с этим, по состоянию на апрель 2018 года, реализация права на портативность данных в том виде, в котором оно представлено в Регламенте, отсутствует (ввиду невступления в силу Регламента), однако при осуществлении практического анализа, представляется, что право на переносимость данных используется, и, как отмечается Рабочей группой по статье 29, уже существует в других областях правового регулирования (расторжение договорных отношений, роуминг, трансграничный доступ к услугам) [5, стр. 4].

Использование права на портативность личных данных осложняется различным подходом к обработке информации. Регламент не обязывает контроллеров структурировать данные в одинаковой форме, и в связи с этим, необходимо понимать, что реализация права на портативность данных с большой долей вероятности будет осложнена на практике по причине существования разнообразных подходов к организации и структурированию информации. Но в то же самое время, такая ситуация открывает потенциал для сотрудничества между участниками рынка и возможное повышение качества предоставляемых услуг.

Сущность права на портативность данных в ближайшее время будет постоянно видоизменяться по причине появления и развития правоприменительной практики напрямую связанных с ним элементов, в особенности, выражения согласия субъекта на обработку его / её личных данных.

В Латвии на настоящий момент, новый нормативный акт о защите личных данных (заменяющий закон о защите данных физических лиц) ещё не принят, но уже находится на стадии принятия. 06 марта 2018 года, проект закона об обработке личных данных (Personas datu apstrādes likums) был рассмотрен и поддержан в Кабинете Министров [6, пар. 40].

В законопроекте DVI упоминается как компетентное надзорное учреждение, учреждённое в соответствии со статьёй 51 Регламента, целью которого будет содействовать постоянному применению Регламента в рамках ЕС, а потому значительная часть толкования Регламента в перспективе латвийского правового поля будет осуществляться именно сотрудниками DVI.

Также, стоит отметить, что по состоянию на 26 апреля 2018 года, в законопроекте не присутствует упоминание о праве на портативность данных, однако это не означает, что на территории Латвии не будет допустимо его применение, поскольку Регламент обладает прямой и обязательной силой применения [4, ст. 288].

Список использованых источников

1. Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L 281/50 (23/11/1995).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119/1 (04/05/2016).
3. A Digital Single Market Strategy for Europe – Analysis and Evidence. European Commission staff working document. Available at: http://ec.europa.eu/priorities/digital-single-market/index_en.htm.
4. The Treaty on the functioning of the European Union. International treaty amended by the Treaty of Lisbon, adopted 2007, 13th December and published in consolidated version in the Official Journal of the European Union C 326/47 (26/10/2012).
5. Article 29 Working Party - Guidelines on the right to data portability. Adopted on 2016, 13th December, and revised on 2017, 5th April. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
6. Latvijas Republikas Ministru Kabineta sēdes protokols Nr. 14 no 2018. gada 06. marta. Publicēts: http://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2018-03-06

References:

1. Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L 281/50 (23/11/1995).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119/1 (04/05/2016).
3. A Digital Single Market Strategy for Europe – Analysis and Evidence. European Commission staff working document. Available at: http://ec.europa.eu/priorities/digital-single-market/index_en.htm.
4. The Treaty on the functioning of the European Union. International treaty amended by the Treaty of Lisbon, adopted 2007, 13th December and published in consolidated version in the Official Journal of the European Union C 326/47 (26/10/2012).

5. Article 29 Working Party - Guidelines on the right to data portability. Adopted on 2016, 13th December, and revised on 2017, 5th April. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
6. Meeting protocol Nr. 14 of the Cabinet of Ministers (2018, 06th March). Available in latvian language at: http://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2018-03-06