ИНСТИТУТ ИССЛЕДОВАНИЙ ИНТЕРНЕТА

РИФ- 2018

Регламент (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц относительно обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент по защите персональных данных)»

27 апреля 2016 г.

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.

Правовая система Европейского Союза

- **Нормативно-правовой механизм**:

  - «первичное право» (Маастрихтский договор, Римский договор, Европейская Хартия об основных правах)

  - «вторичное право» (регламенты, директивы, решения, рекомендации и заключения),

  - прецедентное право Суда Справедливости Европейского Союза (*Court of Justice of the European Union, CJEU*)

- **Институциональный механизм:**

  - Европейский Парламент,

  - Европейский Совет,

  - Европейская Комиссия,

  - Суд Справедливости Европейского Союза

Основные причины принятия Общего Регламента GDPR

- **24 октября 1995 г.** принята Директива 95/46/ЕС Европейского парламента и Совета о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (**Директива 95/46/ЕС**)
- «Опосредованная» применимость Директивы 95/46/ЕС вызвала фрагментацию и противоречия в национально-правовом регулировании порядка и уровня защиты данных в государствах-членах Евросоюза, связанные с имплементацией и применением **Директивы 95/46/ЕС,** а также в правоприменительной практике.

Примеры расхождений применения штрафных санкций, связанных с защитой персональных данных в государствах-членах ЕС

- в Германии компания «LIDL» оштрафована на **1,460, 000 €** (2008 г.);
- в Италии компания «Google» оштрафована на **1,000,000 €** (2013 г.);
- в Великобритании компания «TalkTalk» оштрафована на **400 000 £** (2016 г.).
- Испании компания «Facebook» оштрафована на **1,200,000 €** (2017 г.)
- В большинстве стран-членов Евросоюза размеры штрафов значительно меньше, например: в Латвии – **4,248 €;** в Словакии – **8,000 €;** в Польше – **47,000 €.**

Основные причины принятия Общего Регламента GDPR

- Стремительные технологические изменения, глобализация и потребности развития единого цифрового рынка в Европейском Союзе
- Увеличение объема предоставления физическими лицами персональных данных (добровольно, публично и в глобальном масштабе) государственным органам и частным компаниям для их использования при осуществлении ими своей деятельности;
- Трансграничное перемещение/обмен персональных данных между государственными и частными структурами в Европейском Союзе, в т.ч. между физическими лицами;
- Обеспечение защиты персональных данных физических лиц со стороны государственных и частных структур в рамках Евросоюза;
- Обеспечение юридической однозначности контроля со стороны физических лиц обработки и использования своих персональных данных.

Цели принятия Общего Регламента GDPR

- Необходимость устранения различий и противоречий в уровне и порядке защиты прав физических лиц в связи с обработкой персональных данных и отмена Директивы 95/46/ЕС;
- Гармонизация/унификация национально-правового правового регулирования и правоприменительной практики в сфере защиты прав и свобод физических лиц в отношении обработки их персональных данных независимо от гражданства и местожительства физических лиц;
- Создание единообразного общеевропейского нормативно-правового механизма защиты прав физических лиц в отношении обработки их персональных данных, независимо от гражданства и местожительства физических лиц
- Создание общеевропейского институционального механизма защиты прав и свобод физических лиц в отношении обработки их персональных данных

Сроки и параметры применения Общего Регламента GDPR

- **24 мая 2016 г. вступил в силу ;**
- **с 25 мая 2018 г. будет применяться в полном объеме:**

- непосредственное применение в рамках национального права государств-членов Евросоюза, включая правоприменительные органы;

- «приоритетный эффект» действия в случаях «конфликта» между национальным правом и Общим Регламентом GDPR;

- непосредственное применение Судом Справедливости Европейского Союза

Территориальное и юрисдикционное действие Общего Регламента GDPR

(Статья 3)

- Территориальная сфера применения ограничивается переделами Европейского Союза,
- Юрисдикционная сфера действия распространяется в т.ч. на лиц, не учрежденных Европейском Союзе и находящихся за его пределами

Юрисдикционная сфера действия Общего Регламента GDRP

- Распространяется на лиц, не учрежденных и находящихся за пределами Европейского Союза если они обрабатывают персональные данные субъектов данных в Евросоюзе:

1) в связи с предложением товаров или услуг субъектам данных в Евросоюзе, независимо от того связано это с оплатой товаров или услуг или нет;
2) в связи с мониторингом действий/поведения субъектов данных в Евросоюзе постольку, поскольку их действия совершаются на территории Евросоюза.

Признаки, подтверждающие намерение предлагать товары или услуги субъектам данных в Евросоюзе

- использование языка или валюты, обычно применяемых в одном или нескольких странах-членах ЕС;
- возможность заказать товары и услуги на этом языке в зоне национальных доменов верхнего уровня Евросоюза и стран-членов ЕС («.de», «.fr», «.eu» и др.).
- упоминание потребителей/пользователей, которые находятся в Евросоюзе

Мониторинг действий/поведения субъектов данных в Евросоюзе

- Контроль действий субъекта данных в Евросоюзе включая: составление профиля физического лица, в частности, для принятия решений относительно анализа либо прогнозирования ее/его личных предпочтений, особенностей поведения, а также личностных характеристик.

Понятие обработки персональных данных

- **«обработка» (*processing*)** – означает любую операцию или набор операций, которые совершаются с персональными данными или набором персональных данных, с использованием автоматизированных средств и без таковых, в числе которых сбор, запись, организация, структурирование, хранение, переработка или изменение, поиск и выборка, экспертиза, использование, раскрытие посредством передачи, рассылка или иной способ предоставления для доступа, группировка или комбинирование, отбор, стирание или уничтожение

Круг ключевых лиц обработки персональных данных

- Контроллер (*Controller*);
- Обработчик (*Processor*);
- Субъект персональных данных

Круг ключевых лиц обработки персональных данных

- **Контроллер** – физическое или юридическое лицо, государственный орган, агентство или иной орган, который самостоятельно или совместно с другими, определяет цели и средства обработки персональных данных (п.7 Ст.4);
- **Обработчик** – физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные *от имени и по поручению Контроллера* (п.7 Ст.4)

Круг ключевых лиц обработки персональных данных

- **Контроллер или обработчик** не учрежденнные в Евросоюзе и находящихся вне его территориальных пределов, но обрабатывающие персональные данные физических лиц в Евросоюзе должны назначить представителя в Евросоюзе

  (п.1 ст. 27)

Контроллер vs. Обработчик
Controller vs. Processor

- Различие между контроллером и обработчиком – важн*о* в силу их предметной и функциональной компетенции, мер ответственности и т.д.
- Контроллер данных – ключевая сторона, обязанности которой охватывают, в частности, получение согласия от субъекта персональных данных на их обработку, операции по отзыву согласия, предоставление права/запрет права доступа к данным и т.д. Например, субъект персональных данных, хочет отозвать согласие на обработку своих данных (удалить данные) и обращается к Контроллеру с запросом. Даже если такие данные хранятся на серверах обработчика, Контроллер обеспечивает удаление отзываемых персональных данных с сервера обработчика.

Принципы защиты персональных данных

(Статья 5)

- **правомерность, справедливость и открытость/траспаренность** (*lawfulness, fairness and transparency*) – персональные данные должны обрабатываться на законных основаниях, справедливым и открытым образом в отношении субъекта данных;
- **целевое ограничение обработки** персональных данных (*purpose limitation*) – сбор и обработка персональных данных осуществляется для конкретных, ясных и законных целей, без их дальнейшей обработки способами, несовместимыми с этими целями;
- **минимизация данных** (*data minimisation*) – достоверность персональных данных и их соответствие целям для которых они обрабатываются;
- **точность** персональных данных (*accuracy*) – персональные данные должны быть точными, своевременно обновляемыми, удаляемыми, исправляемыми с учетом целей, для которых они были обработаны;
- **ограничение хранения** персональных данных (*storage limitation*) – персональные данные должны храниться в форме, позволяющей идентифицировать субъектов данных, в течение срока, необходимого для целей, для которых персональные данные обработаны;
- **целостность и конфиденциальность** персональных данных (*integrity and confidentiality*) – обработка персональных данных должна осуществляться способом, обеспечивающим их безопасность, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, повреждения или уничтожения, с использованием соответствующих технических и организационных мер.

Принципы защиты персональных данных
(п.2. Статьи 5)

- **подотчетность Контроллера** (*Controller accountability*) – ответственность Контроллера за соблюдение принципов GDPR, который должен обязан дать соответствующее подтверждение

Понятие персональных данных

- **«Персональные данные» (*personal data*)** – означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в интернете (онлайн-идентификатор) или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица (п.1.ст.4).

Категории персональных данных

Особые категории («конфиденциальные») персональных данных («*sensitive data*»): расовое/этническое происхождение; политические убеждения; религиозные или философские убеждения; членство в профсоюзах; генетические данные; биометрические данные, идентифицирующие физическое лицо; данные о здоровье; данные о половой жизни/сексуальной ориентации

Обще правило: обработка особых категорий персональных данных запрещена, но их обработка возможна если:

- конфиденциальные данные находятся в открытом доступе;
- на их обработку получено явно выраженное согласие физического лица;
- такая обработка законодательно предусмотрена для конкретных целей и связана с общественными интересами или здравоохранением;
- право закрепляет надлежащие гарантии при обработке таких данных и если они связаны со сферой общественного здравоохранения, занятости и социальной защитой.

Согласие субъекта данных на обработку

- **«согласие»** (*consent*) – субъекта данных означает любое свободно данное, конкретное, осознанное и однозначное идентифицируемое желание субъекта данных, посредством которого он/она путем заявления, либо ясным утвердительным действием, выражает согласие на обработку персональных данных, относящихся к нему/к ней;

Права субъекта персональных данных
(Глава III)

- Право на исправление данных
- Право на удаление данных («право на забвение»)
- Право на ограничение обработки
- Право на переносимость данных
- Право на возражение
- Право на доступ к данным
- Право на получение информации об утечке данных
- Право подавать жалобу в надзорный орган
- Право на эффективные средства судебной защиты против надзорного органа
- Право на эффективные средства судебной защиты в отношении контроллера или обработчика
- Право действовать через представителя
- Правом на получение компенсации от контроллера или обработчика за полученный ущерб.

Институциональный механизм Европейского Союза в сфере защиты персональных данных

Общеевропейский регуляторный уровень

- **Группа *WP29*** (создана в соответствии со статьей 29 Директивы 95/46/ЕС) действует до 25 мая 2018г.
- **Европейский совет по защите данных** (*European Data Protection Board, EDPB)* – новый директивный и надзорный орган с правами юридического лица, заменяющий с 25 мая 2018 г. Группу *WP29*
- **Европейский инспектор по защите данных** (*European Data Protection Supervisor*) и его персонал;

Институциональный механизм Европейского Союза в сфере защиты персональных данных

Общеевропейский регуляторный уровень

- **Европейская Комиссия** (компетентна принимать подзаконные акты, связанные с Общим Регламентом GDPR (в порядке Регламента 182/2011/ЕС Европейского Парламента и Совета от 16 февраля 2011 г. об определении правил и общих принципов, связанных с механизмами контроля со стороны государств-членов за осуществлением Европейской Комиссией ее полномочий по принятию имплементирующих актов);
- **Европейский Парламент и Совет** (получают отчеты Европейской Комиссии, начиная с 25 мая 2020 г. и **каждые 4 года** в последующем, об оценке и анализе применения Регламента GDPR; получают **ежегодные отчеты** Европейский совет по защите данных (*EDPB*);
- **Суд Справедливости Европейского Союза** (*Court of Justice of the European Union, CJEU)*

Надзорный механизм Европейского Союза в сфере защиты персональных данных

Общеевропейский регуляторный уровень

Европейский Совет по защите данных (*EDPB*)

- В состав входят руководители одного надзорного органа каждого государства-члена, Европейский инспектор по защите данных (или их представители), представитель Европейской Комиссии
- Составляет ежегодный отчет о защите персональных данных физических и их обработки в Евросоюзе, включая третьих страны и международные организации
- Ежегодный отчет публикуется в открытом доступе
- Ежегодный отчет передается Европейскому Парламенту, Совету и Европейской Комиссии.

Надзорный механизм Европейского Союза в сфере защиты персональных данных

Общеевропейский регуляторный уровень

- **Европейский инспектор по защите данных**

(Регламент 45/200/EC1 Европейского Парламента и Совета от 18 декабря 2000 г. о защите физических лиц в сфере обработки персональных данных институтами и органами Сообщества, а также о свободном перемещении таких данных - *Regulation (EC) No 45/2001 of the European Parliament and of the Council, of December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*).

- **Группа *WP29*** 11 апреля 2018 (*Brussels*) приняла решение создать **Рабочую группу по соцсетям** (*Social Media Working Group*), которая наряду с **Европейским советом по защите данных (*EDPB)*** будет содействовать после 25 мая 2018 г. согласованному применению Общего Регламента GDRP

Надзорный механизм Европейского Союза в сфере защиты персональных данных

Национальный регуляторный уровень («внесудебный»)

- **Национальный надзорный орган/органы** (*supervisory authority)*

Каждое государство-член ЕС:

- должно учредить один или несколько полномочных государственных органов с **самостоятельным статусом**, ответственных за мониторинг применения Общего Регламента GDRP для обеспечения защиты прав физических лиц в отношении обработки персональных данных и их свободного движения на территории Евросоюза

- уведомить Европейскую Комиссию об учреждении Надзорного органа/органах;

- обеспечить сотрудничество Надзорного органа/органов между собой, с Европейской Комиссией и Европейским Советом по защите данных (*EDPB*)

- **Инспектор по защите персональных данных** (*Data Protection Supervisor*), назначаемый контроллером и обработчиком

Национальные надзорные органы стран-членов Европейского Союза

- **Австрия -** Орган по надзору за соблюдением законодательства о защите персональных данных (*Österreichische Datenschutzbehörde*);
- **Бельгия -** Комиссия по защите неприкосновенности частной жизни (*Commission de la protection de la vie privée*);
- **Болгария -** Комиссия по защите персональных данных (*Commission for Personal Data Protection*);
- **Великобритания -** Управление комиссара по информации (*The Information Commissioner's Office*).
- **Венгрия -** Национальное управление по защите данных и свободе информации (*National Authority for Data Protection and Freedom of Information*);
- **Кипр -** Уполномоченный по защите персональных данных (*Commissioner for Personal Data Protection*);
- **Дания** - Агентство по защите персональных данных (*Datatilsynet*);

Национальные надзорные органы стран-членов Европейского Союза

- **Финляндия -** Управление Омбудсмена по защите данных (*Office of the Data Protection Ombudsman*);
- **Франция -** Национальная комиссия по информатике и свободам (*Commission Nationale de l'Informatique et des Libertés, CNIL*);
- **Германия -** Федеральный комиссар по защите данных и свободе информации (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*);
- **Греция -** Управление защиты данных (*Hellenic Data Protection Authority*);
- **Ирландия -** Комиссар по защите данных Ирландии (*Data Protection Commissioner*);
- **Испания -** Агентство по защите данных Испании (*Agencia de Protección de Datos*);
- **Италия -** Комитет по защите прав субъектов персональных данных (*Garante per la protezione dei dati personali*);

Национальные надзорные органы стран-членов Европейского Союза

- **Латвия -** Государственная инспекция по данным (*Data State Inspectorate*)
- **Литва -** Государственный орган по защите данных (*State Data Protection*)
- **Люксембург -** Национальная Комиссия по защите данных (*Commission Nationale pour la Protection des Données*)
- **Мальта -** Управление Комиссара Мальты по защите данных (*Office of the Data Protection Commissioner*);
- **Нидерланды -** Управление по защите персональных данных (*Autoriteit Persoonsgegevens*);
- **Польша -** Бюро Генерального инспектора по защите персональных данных (*The Bureau of the Inspector General for the Protection of Personal Data, GIODO*);
- **Португалия -** Национальная комиссия по защите данных (*Comissão Nacional de Protecção de Dados, CNPD*);

Национальные надзорные органы стран-членов Европейского Союза

- **Румыния -** Национальный надзорный орган по обработке персональных данных (*The National Supervisory Authority for Personal Data Processing*);
- **Словацкая Республика -** Управление по защите персональных данных (*Office for Personal Data Protection of the Slovak Republic*);
- **Словения -** Комиссар по информации Словении (*Information Commissioner*);
- **Швеция -** Инспекция по надзору за данными Швеции (*Datainspektionen*);
- **Хорватия -** Агентство по защите персональных данных (*Croatian Personal Data Protection Agency*);
- **Чешская Республика -** Управление по защите персональных данных (*Urad pro ochranu osobnich udaju*);
- **Эстония -** Инспекция по защите персональных данных (*Andmekaitse Inspektsioon*);

Уведомление об утечке персональных данных

- **Контроллер** уведомляет компетентный **надзорный орган** без неоправданной задержки в течение **72 часов** после того, как он узнает об утечке персональных данных
- **Контроллер** сообщает **субъекту данных** об утечке персональных данных, без неоправданной задержки в случаях, когда утечка персональных данных, вероятнее всего приведет к высокому риску для прав и свобод физических лиц;
- **Обработчик** уведомляет **Контроллера** без неоправданной задержки об утечке персональных данных как только ему стало известно об утечке персональных данных.

Ответственность, средства правовой защиты, санкции (Глава VIII).

- **Общая** ответственность контроллера и обработчика
- **Ответственность контроллера** (соблюдение принципов обработки; проведение оценки воздействия на защиту данных; ответственность за ущерб, вызванный обработкой данных; за утечку данных; несоблюдение предписаний надзорных органов и т.д.)
- **Ответственность обработчика** (общая и договорная): за утечку данных, за несоблюдение кодексов поведения, утвержденного механизма сертификации, ответственность за ущерб, вызванный обработкой данных; предписаний контроллера и надзорных органов и т.д.)

Общие условия наложения административных штрафов

Надзорный орган обеспечивает эффективность, соразмерность/пропорциональность и сдерживающее воздействие наложения административных штрафов (Статья 83).

- **Административные штрафы в размере до 10 000 000 €** или применительно к хозяйствующему субъекту, в размере до 2% от «обще-странового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше за нарушения:

(a) обязательства контроллера и обработчика в соответствии со Статьями 8, 11, 25-39 и 42 и 43;

(b) обязательства органа сертификации (ст.ст. 42 и 43);

(c) обязательства органов, надзорного органа (ст. 41 (4).

Общие условия наложения административных штрафов

- **Административные штрафы** до **20 000 000 €** или применительно к хозяйствующему субъекту в размере до 4% от «обще-странового» годового оборота за весь предыдущий финансовый год, в зависимости от того, какая сумма больше за нарушения:

(a) нарушение основных принципов обработки, в том числе условий, в отношении согласия (ст.ст. 5, 6, 7 и 9);

(b) прав субъектов данных, предусмотренных (ст.ст. 12-22);

(c) передачи персональных данных получателю в третьей стране или международной организации (ст. ст. 44-49);

(d) любых обязанностей в соответствии с правом государства-члена, принятому в рамках Главы IX;

(e) несоблюдения предписания, или временного или окончательного ограничения на обработку, или приостановление потоков данных надзорным органом (ст. 58 (2), либо отказ в предоставлении доступа в нарушение ст. 58 (1).

Общие условия наложения административных штрафов

- **Административные штрафы** в размере до **20 000 000 €** или, применительно к хозяйствующему субъекту, в размере до 4% от «обще-странового» годового оборота хозяйствующего субъекта за весь предыдущий финансовый год, в зависимости от того, какая сумма больше за нарушения предписаний надзорного органа (ст. 58 (2)).

Санкции

- Государства-члены вправе устанавливать нормы относительно иных санкций за нарушения Общего Регламента GDRP
- Государства-члены должны уведомить Европейскую Комиссию о принятии соответствующих нормативно-правовых положений норм до 25 мая 2018 г., а также незамедлительно уведомляют о любых последующих изменениях, затрагивающих такие положения.

РИФ- 2018

ИНСТИТУТ ИССЛЕДОВАНИЙ ИНТЕРНЕТА

СПАСИБО ЗА ВНИМАНИЕ!

Касенова Мадина
(д.ю.н., профессор Московской высшей школы социальных и экономических наук)

Институт Исследований Интернета (ИИИ) содействует решению практических вопросов реализации Общего Регламента GDRP https://internetinstitute.ru/