GDPR

С ЕДИН ПОГЛЕД

СПЕЦИАЛНО ИЗДАНИЕ НА Novatel

Deutsche Telekom Group

GDPR С ЕДИН ПОГЛЕД

СПЕЦИАЛНО ИЗДАНИЕ НА НОВАТЕЛ БЪЛГАРИЯ

Съдържание

ВЪВЕДЕНИЕ **3**

КАКВО Е GDPR? **4**

КАКВО ЩЕ СТАНЕ, АКО НЕ СПАЗИМ ИЗИСКВАНИЯТА НА GDPR? **5**

ЗАЩО ЕС РЕШИ ДА СЪЗДАДЕ GDPR? **6**

ВЪВЕДЕНИЕ В GDPR **7**

Права на гражданите на ЕС 7
Принципите на GDPR 7

ЛИЧНИТЕ ДАННИ **8**

Какво означава „лични данни“? 8
Чувствителни лични данни 8
Най-важното за личните данни 9
Изначална защита на личните данни и защита по подразбиране 10
Длъжностно лице по защита на данните 10
Нарушаване на данни 11

ПРАВОТО ДА БЪДЕШ „ ЗАБРАВЕН“ **13**

ОДИТ НА СЪОТВЕТСТВИЕТО И ВОДЕНЕ НА ЗАПИСИ **15**

ЗА НОВАТЕЛ **16**

ЗАКЛЮЧЕНИЕ **17**

Въведение

GDPR е една от най-актуалните теми през последните няколко месеца. И с право. Очаква се тази нова Европейска регулация да повлияе сериозно върху почти всички бизнеси и организации, които работят с лични данни под една или друга форма.

Интересното е, че GDPR има два главни аспекта – юридически и технически.

От една страна са юридическите изисквания, наложени от регламента – изискванията. От друга – стои въпросът как тези изисквания ще бъдат приложени в реалния живот и бизнес.

Ние от Новател също ще бъдем засегнати от влизането в сила на GDPR. Ние също работим с данни на наши клиенти и ще се наложи да съгласуваме нашите политики и практики с GDPR.

Това, което ни дава важно предимство и улеснява задачата е, че ние сме технологична компания и разполагаме с необходимата технологична инфраструктура да реализираме тези изисквания.

И вече го направихме. Няколко месеца преди влизането в сила на Регламента.

И искаме да споделим своя опит.

Смятаме да го направим в специално подготвен за целта уебинар този месец, който ще обявим допълнително.

А, като начало, подготвихме една кратка брошура, която да ви даде бърз, но качествен поглед относно темата за GDPR. Така ще можем да сме „на една страница“, когато дойде денят на уебинара.

Очакваме вашите въпроси и коментари на marketing@novatel.bg.

Приятно четене!

Какво е GDPR?

GDPR е съкращение от General Data Protection Regulation. Този регламент на Европейския съюз се очаква да промени коренно начина по който бизнеса борави с личните данни на своите клиенти и партньори.

Регламентът установява правилата относно защитата на физическите лица по отношение на обработката на лични данни и правилата, свързани със свободното им движение. По този начин, регулацията защитава основните права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

За да се покрият изискванията на тази регулация, обаче, фирмите ще трябва да съобразят всички правни аспекти и, в същото време, да намерят техническо решение на казуса – как да бъдат наистина приложени на практика тези изисквания.

Какво ще стане, ако не спазим изискванията на GDPR?

До 25 май 2018 г. бизнесът трябва да приложи новата регулация в дейността си и в случай на неспазване правилата може да бъде наложена глоба до 20 милиона евро или 4% от годишния оборот.

Общият регламент за защита на данните (GDPR) е един от най-противоречивите и очаквани законодателни актове, замислени в ЕС през последните години.

Това е промяна в играта на бизнеса, тъй като е свързана с рисковете при защитата на данните - и по-важното - нарушаването им.

Защо ЕС реши да създаде GDPR?

Настоящото законодателство, директивата за защита на данните (95/46/ЕО), бе договорено през 1995 г., преди приемането на интернет и World Wide Web и повече от 10 години преди създаването на Facebook и Twitter.

Светът се промени, но законодателството за защита на данните - не.

Освен това съществуващите правила се основават на директива, чието значение е, че всяка от 28-те държави-членки на ЕС тълкува и прилага правилата по свой начин.

Европейската комисия изложи през 2012 г. своите принципи за защита на данните и проекта за нов регламент.

Наредбата ще се прилага еднакво и едновременно към 28-те държави-членки след нейното приемане.

След повече от три години дискусия и дебат, окончателната версия на GDPR беше договорена през май 2016 г.

Новият регламент ще влезе в сила на 25 май 2018 г.

Въведение в GDPR

Права на гражданите на ЕС

В основата на GDPR е целта да се определят правата за защита на данните, които се предоставят на всички граждани на ЕС. Регулирането е съсредоточено върху налагането на тези права, без значение коя организация обработва личните данни на гражданите или къде се провежда.

Поради това основните елементи на GDPR детайлизират редица "Права на гражданите на ЕС" по отношение на начина, по който се използват техните лични данни. Списъкът е разширен и ще изисква значителни промени в приложенията, политиките и процедурите за постигане на съответствие.

Принципите на GDPR

Освен правата на гражданите, GDPR определя набор от "принципи", които регулират цялата обработка на лични данни. Идеята е да се определят условията, при които обработката на данни е разрешена. Ако дадена организация не може да покаже, че работи в тези условия, тогава нейните дейности могат да се считат за незаконни съгласно GDPR.

Основен принцип е, че данните могат да се събират само "за конкретни, изрични и легитимни цели", което означава, че няма да бъде приемливо първо да се събират данни и да се решава впоследствие как може да се използват.

Освен това може да се събира само минималното количество данни, необходимо за изпълнение на тези задачи. Организациите не могат да съхраняват данните във формат, който позволява лесно идентифициране на участващите, след като информацията вече не е необходима за първоначалната цел.

Личните данни

Какво означава „лични данни“?

Най-често срещаното и полезно обяснение е: "всякаква информация, свързана с идентифицирано или подлежащо на идентификация физическо лице".

Идентификацията може да бъде пряка или непряка и включва такива идентификатори като "име, идентификационен номер, данни за местоположението, онлайн идентичност, един или повече фактори, специфични за физическото, физиологичното, генетичното, умственото, културното или социалното му идентифициране", но също така включват оценяване на представянето на дадено лице на работното място, икономическа ситуация, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движения.

Дефиницията е технологично неутрална.

Няма значение как се съхраняват личните данни - на хартия, на информационна система, на система за видеонаблюдение и т.н.

Чувствителни лични данни

Чувствителните лични данни са лични данни, съдържащи информация за:

- Расов или етническия произход на субекта на данните.
- Религиозните му убеждения или други подобни убеждения.
- Политически разбирания.
- Дали е член на профсъюз (по смисъла на Закона за синдикалните и трудовите отношения от 1992 г.).
- Физическото или психическото му състояние.
- Неговият сексуален живот.

- Всяко производство за всяко престъпление, извършено или предполагаемо извършено от него, разпореждането с това производство или присъдата на който и да е съд в това производство.

Най-важното за личните данни

Личните данни трябва да бъдат:

- Обработвани законно, справедливо и по прозрачен начин по отношение на субекта на данните ("законност, справедливост и прозрачност").

- Събрани за конкретни, изрични и законни цели и не се обработват по начин, който е несъвместим с тези цели; по-нататъшна обработка за целите на архивирането в интерес на обществото, научни или исторически научни цели.

- Адекватни, уместни и ограничени до това, което е необходимо във връзка с целите, за които се обработват ("минимизиране на данните").

- Точни и, когато е необходимо, актуализирани; трябва да се предприемат всички разумни стъпки, за да се гарантира, че личните данни, които са неточни, незабавно ще бъдат изтрити или отстранени ("точност").

- Съхранявани във форма, която позволява идентифициране на субектите на данни не по-дълго от необходимото за целите, за които се обработват личните данни; личните данни могат да бъдат съхранявани за по-дълги периоди, единствено с цел архивиране за обществени интереси, научни или исторически научни цели или статистически цели.

Изначална защита на личните данни и защита по подразбиране

Вземайки предвид състоянието на техниката, разходите за изпълнението и естеството, обхвата, контекста и целите на обработката, както и рисковете от различна вероятност и тежест за правата и свободите на физическите лица, породени от обработката, администраторът, както по време на определянето на средствата за обработка, така и по време на самата обработка, трябва да приложи подходящи технически и организационни мерки, като например *псевдонимизиране*.

Предвижда се да се прилагат различни принципи за защита на данните, като например минимизиране на данните, и да се интегрират необходимите предпазни мерки в обработката, за да се отговори на изискванията на бъдещия регламент и да защитят правата на субектите на тези данни.

Контролният орган прилага подходящи технически и организационни мерки, за да гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка специфична цел на обработката.

Това задължение се отнася до количеството събрани лични данни, степента на тяхната обработка, периода на тяхното съхранение и достъпа им**.**

Длъжностно лице по защита на данните

Ако е необходимо, трябва да определите длъжностно лице по защита на данните (ДЗД) или някой, който да поеме отговорност за спазването на защитата на данните. Трябва да се прецени къде тази роля ще се намира в структурата и управлението на вашата организация

Контролиращият орган и администраторът на лични данни гарантират, че служителят по защита на данните е въвлечен, надлежно и своевременно във всички въпроси, свързани със защитата на личните данни.

GDPR ще изисква от някои организации да определят служител по защита на данните, например публични органи или такива, чиито дейности включват редовен и систематичен мониторинг на субектите на данни в голям мащаб.

Важното е да се уверите, че този човек – било то някой от вашата организация или външен консултант по защита на данните, поема правилно отговорността за спазването на изискванията за защита на данните и има знанията, подкрепата и правомощията да прави ефективно.

Затова трябва добре да се обмисли дали да посочите външно ДЗД и ако е така, да прецените дали настоящият ви подход към спазването на изискванията за защита на данните ще отговаря на изискванията на GDPR.

ДЗД се отчита пред ръководството, но се очаква да работи независимо в организационната структура. Основната му задача е защитата на данните и осигуряването на съответствие.

ДЗД е лицето, което ръководи и контролира всички дейности по защита на данните в рамките на даденото дружество.

ДЗД поддържа информирането на управлението по отношение на задълженията им по регламента и е основната точка за контакт на надзорните органи.

Нарушаване на данни

Трябва да сте сигурни, че имате правилните процедури за откриване, докладване и разследване на нарушаване на лични данни.

В случай на нарушаване на лични данни администраторът уведомява компетентния надзорен орган в съответствие с член 55 без ненужно забавяне и, ако е възможно, не по-късно от 72 часа след като е узнал за него.

Уведомлението трябва да:

- описва естеството на нарушението на личните данни, включително категориите и приблизителния брой на засегнатите субекти на данни, както и категориите и приблизителния брой записи на лични данни;

- съобщава името и данните за контакт на служителя за защита на данните или на друго звено за контакт, където може да се получи повече информация;

- описва вероятните последици от нарушаването на личните данни.

Когато нарушаването на личните данни може да има последствия върху правата и свободите на физическите лица, администраторът съобщава за нарушението на личните данни на субекта възможно най- бързо.

Правото да бъдеш „ забравен“

Правото на изтриване е известно също като "правото да бъдеш забравен".

Широкият принцип, на който се основава това право, е да даде възможност на дадено лице да поиска заличаване или премахване на лични данни, когато няма причина за продължаване на съществуването им в базата данни.

Субектът на данните има право да получи от администратора правото на изтриване на лични данни, които се отнасят до него, без ненужно забавяне и администраторът е длъжен да изтрие личните данни без неоправдано забавяне.

Правото на изтриване не предоставя абсолютно "право да бъдеш забравен". Лицата имат право да изтрият личните данни и да предотвратят обработката при следните обстоятелства:

- Когато личните данни вече не са необходими във връзка с целта, за която са били първоначално събрани / обработени.

- Когато лицето оттегли съгласието си.

- Когато индивидът възразява срещу обработката и няма преимуществен легитимен интерес за продължаване на обработката.

- Личните данни са били незаконно обработени (т.е. по друг начин са в нарушение на GDPR).

- Личните данни трябва да бъдат изтрити, за да се спази правно задължение.

- Личните данни се обработват във връзка с предлагането на услуги на информационното общество на дете.

Има допълнителни изисквания, когато искането за изтриване се отнася до личните данни на деца, което подчертава наблягането на GDPR върху подобрената защита на такава информация, особено в онлайн среда.

Ако обработваните личните данни са на деца, трябва да се обърне специално внимание на съществуващите ситуации, в които детето е дало съгласието си за обработка и по-късно да поискат изтриване на данните (независимо от възрастта към момента на заявката), особено в сайтовете за социални контакти и интернет форум.

Одит на съответствието и водене на записи

Дружествата, обработващи лични данни, са задължени да водят подробна информация за данните, които съхраняват, както и подробности за обработката на тези данни. Трябва да документирате какви лични данни съхранявате, откъде идват и с кого ги споделяте.

Може да се наложи да организирате информационен одит в цялата организация или в определени бизнес области.

За Новател

Новател е основана в края на 2004г. като част от Deutsche Telekom Group. Като член на една от най-големите европейски телекомуникационни компании, Новател предлага конкурентна алтернатива в сферата на телекомуникациите на българския комуникационен пазар. Ние сме водещ национален доставчик, предлагащ на клиентите си широка гама от най-добрите телекомуникационни услуги.

Новател управлява голяма, напълно своя, високотехнологична оптична мрежа с 39 PoP в България. Като част от Deutsche Telekom Group, ние се придържаме към най-високите стандарти в бранша, независимо дали става въпрос за операции, поддръжка или клиентско обслужване.

Базирана на обширен международен опит и солидни компетенции, Новател предлага телекомуникационни услуги на конкурентни цени, главно за бизнес партньори и интернет доставчици в Югоизточна Европа.

Можете да намерите повече информация за нас на нашия **уебсайт**:

http://www.novatel.bg/

Следете ни във **Facebook** на следния адрес:

https://www.facebook.com/novatel.bg/

Можете да ни намерите и в **LinkedIn** тук:

https://www.linkedin.com/company/1840635/

Заключение

GDPR е чувствителна и популярна тема в момента, но ще стане още по-чувствителна и популярна с наближаването на 25-ти май, а и особено след него.

Тъй като ефектът от регулацията ще е върху практически всички бизнеси и организации, работещи с хора, ако вие управлявате или принадлежите към такава организация, важно е да знаете, че е необходимо да се предприемат конкретни стъпки, реални действия, за да се избегнат доста суровите наказания.

Следете своята електронна поща или фейсбук страницата ни за повече информация за датата и часа на провеждане на нашия уебинар, посветен на опита на нашия екип с GDPR и как приведохме процедурите и политиките на компанията си в съгласие с изискванията на General Data Protection Regulation.