Как да осигурим съответствие с GDPR

telelink

Съдържание

Имате ли цялостен подход към осигуряването на съответствие с изискванията на Общия регламент относно защитата на данните (GDPR)?

Знаете ли кои части от проекта за съответствие може да възложите на външна организация и какви технически мерки могат да бъдат използвани, за да се автоматизира това съответствие?

Предговор

Описаният тук подход осигурява най-пълно съответствие с изискванията на Общия регламент относно защитата на данните (GDPR и/или „Регламентът“) и минимизира риска от глоби. Едновременно с това подпомага организациите да вземат решение как икономически ефективно да въведат необходимите мерки, съобразно техните индивидуални особености.

На база опита и експертизата на екипа ни Телелинк улеснява и ускорява постигането на съответствие на всяка стъпка от проекта за съответствие с GDPR.

1.

Какво представлява Общият регламент относно защитата на данните (GDPR)?

Общият регламент относно защитата на данните (GDPR) е европейски регламент в сила от 25.05.2018 г., предназначен да установи единна рамка за защита на личните данни на гражданите на Европейския съюз.

Целта на Регламента е да защити личните данни на гражданите на ЕС, като налага прозрачност и сигурност в използването им, за да може да се изгради високо ниво на доверие на потребителите в начина, по който техните данни ще бъдат използвани, а цялата общност да се възползва максимално и сигурно от възможностите, предлагани от основаната на данни икономика.

GDPR задава нови изисквания за:

- ясно определени права на физическите лица, собственици на лични данни;
- отчетност при работата с лични данни;
- оценки на риска, свързан с данните и предприемане на адекватни мерки за защита;
- правила за уведомяването при нарушения;
- съхранение и контролиране на достъпа до личните данни;
- защита на данните през целия им жизнен цикъл;
- заличаване на данни.

Какъв тип данни са „лични“?

Всяка информация, която може да бъде свързана с идентифицирано физическо лице, представлява лични данни и бива регулирана от GDPR.

Такъв тип идентифициращи данни могат да бъдат срещнати и под термина Personally Identifiable Information – PII. Това включва информация по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на индивида, като например:

- идентификационни номера (ЕГН, телефонен номер, номера на сметки и др.);
- данни за местонахождение (напр. адрес или геолокация);
- онлайн идентификатори (напр. IP адрес, адрес на електронна поща) и много други.

Важно е да се отбележи, че въпреки че няма ясен и краен списък какво са лични данни, всички данни, които могат да бъдат свързани с физическо лице трябва да бъдат защитени адекватно, тоест пропорционално на риска за правата и свободите на физическото лице.

Кой е контролният орган?

В България надзорният орган, отговорен пряко за въвеждането в националното законодателство и прилагането на актовете на Европейската комисия в областта на защитата на личните данни, в това число и за GDPR, е Комисията за защита на личните данни – КЗЛД.

КЗЛД от своя страна участва в Европейския комитет за защита на данните (EPDB), който осигурява еднаквото прилагане на Регламента във всички страни от Европейския съюз.

2.

Как да осигурим съответствие с GDPR?

Проектът за осигуряване на съответствие е комплексен, тъй като обхваща почти всички части от организацията, за да може да се осигури пълно съответствие. Стъпките, изброени по-долу са проектирани именно с тази цел – постигане на ефективно съответствие, без негативно въздействие върху бизнеса.

2.1. Анализ на несъответствията

По време на тази стъпка от проекта трябва да се анализират:

- всички дейности, при които се обработват лични данни, за да се документира основанието за тяхната обработка, както и необходимостта на организацията да обработва тези данни;
- всички бизнес процеси в организацията, за да се осигури пълна видимост върху реално обработваните данни в дружеството и да се положат основите за коректно привеждане в съответствие;
- автоматизираната обработка на лични данни в информационните системи (напр. системите, обработващи данните за заплати, CRM, ERP и др.), като се документират потоците от данни и управлението на достъпа до системи и данни, както и функционалните възможности на системите да осигурят принципите на отчетност и защита.

След като това бъде направено организацията ще разполага с инвентаризация на всички лични данни, които се обработват в момента. На база тази инвентаризация се прави анализ, както спрямо изискванията на Регламента, така и спрямо други нормативни актове, които могат да се отнасят до обработката на лични данни. По този начин се идентифицират всички несъответствия, след което последните могат да бъдат приоритизирани и тяхното цялостно адресиране – планирано.

В резултат от тази стъпка от проекта, организацията трябва да разполага с документирана инвентаризация на обработваните лични данни по бизнес процеси, както и документиран анализ на несъответствията. Идентифицираните несъответствия трябва да са групирани и оценени, както според техния риск, така и според тяхното влияние върху организацията и бизнес процесите.

Ако анализът се извършва от външни консултанти, добър измерител за качеството му е прецизността на извършената работа и съобразяването с особеностите на работа на организацията – нейната структура, бизнес и контекст, в който работи.

Добър индикатор е и включването на юридически анализ, като част от оценката на несъответствията, защото GDPR не съществува във вакуум и има множество други закони и регулации, които поставят изисквания към това какви, как и колко лични данни да бъдат обработвани. Тези изисквания трябва да бъдат взети под внимание и отразени в анализа на несъответствията. От друга страна, съобразяването само с нормативните изисквания, без да се вземат под внимание съществуващите работещи бизнес процеси, може да причини финансови загуби поради неефективност или нарушение на бизнеса.

2.2. Внедряване на процеси и политики

На база анализа на несъответствията се прави анализ за оптимизиране на разходите (cost-benefit analysis). Неговата цел е да установи най-ефективния начин за осигуряване на съответствие.

Следва изготвянето на специализиран план за въвеждане на мерките, който включва разработване и въвеждане на промени в бизнес процесите чрез съставянето на вътрешни политики, правила и промени в документи. Част от тази стъпка по проекта е обучението на ключовите служители относно въведените промени.

В резултат от тази стъпка от проекта, организацията трябва да разполага с добре документирана и структурирана информация за обработваните лични данни в организацията, основанията за тяхното обработване, срокът за тяхното съхранение и други, съгласно изискванията на чл. 30 от Регламента.

Друг индикатор за качеството на разработените и въведените промени, политики и правила за работа с лични данни в организацията, е оказването на минимален негативен ефект върху бизнес процесите и функционирането на организацията, като трябва да бъдат идентифицирани възможности за оптимизация и повишаване на ефективността.

2.3. Внедряване на технологични мерки

При въвеждането на промени в бизнес процесите на организацията се идентифицират тези части и контролни точки, които могат да бъдат автоматизирани чрез технологични решения. Автоматизацията на бизнес процесите може да осигури високо ниво на спазване на Регламента, без да се увеличава административната тежест. За тази цел се изследва кои части от процеси и кои контролни точки могат да бъдат автоматизирани и чрез какви технологични платформи и решения.

След като са идентифицирани конкретни технологични решения и/или модификации на съществуващи технологични системи, се извършва тяхното внедряване. Тези решения и/или модификации обикновено целят да подпомогнат автоматизацията на конкретни дейности по обработка, съхранение и защита на личните данни, както и автоматизация на контролните дейности и най-вече отчетността.

При пристъпване към внедряване се оценяват необходимите ресурси за въвеждането на решенията – финансови, времеви и организационни. Изготвя се пътна карта и проектни планове, обхващайки всички идентифицирани нови технологични решения и промени в съществуващи системи.

Добър измерител за качеството на дейностите в тази част от проекта, особено когато се извършва от външен консултант, е максималното използване на съществуващи технологични решения.

Целта е нови технологии да бъдат въвеждани само там, където са необходими, където са съгласувани с цялостния план за развитие на организацията и където могат да адресират не само конкретните задачи, свързани с GDPR, а и да служат за други цели на организацията, например информационна сигурност, управление на потребителите, управление и анализ на журнални файлове и др.

2.4. Поддържане на съответствието. Ролята на служителя по защита на данните

Важна част от всяко съответствие е, че то не е еднократен акт, а продължителен процес, който изисква наблюдение, оценка и подобрение, съгласно нуждите на организацията и регулацията.

За целта в Регламента изрично се въвежда длъжността „Служител по защита на данните“ или Data Protection Officer, който не бива да бъде в конфликт на интереси с или да бъде част от служителите, натоварени с всекидневните дейности на организацията, като например ИТ директор, главен юрист-консулт, търговски представител, служител в човешки ресурси и др.

Тази роля е задължителна за част от организациите, но не за всички. Там, където не е изрично необходим такъв служител, организацията трябва да вземе решение кой да отговаря за дейностите по поддръжката на съответствието с Регламента. Тези дейности включват:

- Приемане на заявки на клиентите, служители и други субекти, чиито лични данни се обработват, както и на заявките на Комисия за защита на личните данни. Всяка организация взема решение сама за себе си какви канали да използва, но следва да спазва изискването на GDPR тези канали да са съизмерими с начина, по който се комуникира с клиентите по време на всекидневната работа.
- Наблюдение за спазването на GDPR и на други разпоредби за защитата на данните, което може да се осъществи чрез провеждане на ежегоден одит за съответствие. Резултатите от одита трябва да бъдат използвани за подобрение на защитата на личните данни в организацията.
- Препоръки относно оценката на въздействието върху защитата на данните, наблюдаване на извършването на оценката съгласно чл. 35 от GDPR, информиране и напътстване на служителите, извършващи обработване на данни и съблюдаване на изпълнението на техните задължения по силата на Регламента и на други разпоредби за защитата на данни.

Ако тази дейност се възложи на външна организация, добри индикатори за качеството на услугата са: комуникационните канали, които могат да бъдат използвани за подаване на искания, както и каква част от дейностите по обработката на тези искания ще бъде извършена от външната организация. Друг важен индикатор е дали услугата се предлага от едно физическо лице или екип от специалисти, специализирани в отделни направления, като например: юрист, технологичен експерт с добро познаване на информационните системи, в които се обработват лични данни, бизнес аналитик и др.

GDPR предвижда три случая, в които задължително трябва да бъде назначено длъжностно лице за защита на личните данни:

- **обработването се извършва от публичен орган;**
- **когато основната дейност на организацията изисква редовно и систематично мащабно наблюдение;**
- **когато основните дейности на организацията се състоят в мащабно обработване на специални категории данни или на лични данни, свързани с присъди и нарушения.**

Възможно е в ситуации, в които не е задължително да се назначи DPO, все пак такъв да бъде назначен или привлечен отвън, за да улесни комуникацията с клиентите и поддържането на съответствие с GDPR.

3.

Как Microsoft платформите подпомагат отговарянето на изискванията на GDPR?

Един пример за комплексно технологично решение са облачните технологии на Microsoft. Като едни от най-сигурните на пазара, те заемат централно място в голяма част от решенията, които Телелинк предлага:

- Microsoft 365 интегрира в себе си Office 365, Windows 10 и Enterprise Mobility + Security (EMS), които позволяват лесен анализ на текущата инфраструктура и данни, оценка на потенциалните рискове от несъответствие с GDPR, улеснено управление на личните данни, включително тяхната защита от нерегламентирано изтичане.
- Microsoft Compliance Manager е облачно решение, което насочва потребителите чрез съвети и препоръки относно технологичната инфраструктура, необходима за постигане на съответствие. Този инструмент може да се използва за управление на процеса по оценка и управление на риска.
- Адресирането на разпознаването на личните данни и тяхното правилно съхранение може да бъде направено чрез множеството инструменти, интегрирани в Microsoft 365. Тези инструменти дават възможност за класификация на данните, и тяхната защита, предоставяйки решение на основните затруднения в управлението на жизнения цикъл на документите. Това става без значение от използваното място за съхранение на

документите (в облака или в собствена инфраструктура), използваното устройство или приложение.

- Azure Information Protection Scanner дава възможност за създаване на политики за автоматично откриване, класификация и защита на документите в собствена инфраструктура и/или в облака. Azure Information Protection предлага защита на данните, интегрирана в самите файлове, като решението позволява прилагането на различни предефинирани политики за защита на всеки отделен документ. Тази технология позволява криптиране на данните, декриптиране и визуализиране едва след успешно валидиране на лицето, имащо право на достъп.
- Защитата на самото устройство е от особена важност от гледна точка на правилната защита на данните. Windows 10 разполага с множество възможности за защита на информацията, включително и на отделните потребителски профили, които помагат по-добре да защитите цялата информация, обработвана на вашето устройство и в частност да постигнете съответствие с изискванията на GDPR. Windows Hello дава възможност за използване на различни методи за валидиране, като например използване на биометрични данни или multi-factor authentication (MFA). Windows Defender Credential Guard значително повишава защитата срещу всички кибератаки, свързани с кражба на електронна самоличност. В комбинация с Bit Locker и Windows Information Protection важната информация за вашия бизнес остава на сигурно място на самото устройство.

Основни процеси от управлението на информационната сигурност, подпомагащи съответствието с GDPR:

PATCHING AND UPDATING подпомага съответствието с членове 24, 25, 32, 35, 39

NETWORK SECURITY подпомага съответствието с членове 25, 32, 33, 34

ENDPOINT SECURITY подпомага съответствието с членове 18, 24, 25, 32, 35, 39

APPLICATION SECURITY подпомага съответствието с членове 18, 24, 25, 32,34, 35, 39

Речник

Лични данни	данни, които могат да бъдат свързани с идентифициран човек, напр. име, имейл адрес или телефонен номер. Едно лице може да бъде клиент, служител, защитен клиент или друг тип физическо лице. Личните данни могат да бъдат динамични, т.е. да отразяват ситуация в даден момент, както и статични, т.е. да останат същите веднъж създадени.
Чувствителни лични данни	лични данни, които са предмет на повишени защити съгласно законите за защита на личните данни и неприкосновеността на личния живот, напр. данни за раса, етническа принадлежност, политически възгледи, религиозни убеждения, членство в синдикати, здраве, сексуален живот, престъпно поведение или профилиране, финансова документация, биометрична информация (напр. очи, пръстови отпечатъци, разпознаване на глас), биха могли основателно да се считат за особено чувствителни данни.
Обработване на лични данни	“обработване на данни” или “обработване” се отнася по същество до всяко използване на данни, напр. получаване, записване, съхраняване, организиране, адаптиране, промяна, извличане, разкриване или унищожаване.
Субект на личните данни	физическите лица, чиито лични данни се обработват от организацията.