Често задавани въпроси

1. Какво е GDPR?

GDPR е европейски Регламент за защита на личните данни, който влиза в действие от 25.05.2018 г. Предвид това, че е Регламент, той се прилага пряко и в България, т.е. не е необходимо да има местен закон, за да стане Регламентът задължителен за нас.

2. Прилага ли се GDPR за моята компания?

GDPR се прилага за всички компании, които събират и обработват лични данни.

3. Какво са лични данни?

Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признака.
Такива са (примери):

- имена;
- ЕГН;
- адрес;
- телефон;
- месторождение;
- паспортни данни на лицето (физическа идентичност);
- данни относно семейно положение и родствени връзки (семейна идентичност);
- данни относно професионална биография (трудова дейност);
- данни относно здравен статус, психологическо и/или умствено състояние, всякакви други медицински данни;
- данни относно расов или етнически произход, политически, религиозни или философски убеждения, всякакви други данни за обществена идентичност;
- данни относно съдебно минало (свидетелство за съдимост);
- данни относно имотно състояние,
- данни относно финансово състояние, участие и/или притежаване на дялове или ценни книжа на дружества (икономическа идентичност) и др.

4. Основните моменти по GDPR.

- Отчетност - задължението на организациите да спазват закона и да „се отчитат, че го спазват“, т. е. да представят при необходимост документи, доказващи, че законът се спазва. Например ако дадена компания (поради спецификата на бизнес операциите си) взема съгласието за обработка на лични данни по телефона, то в такъв случай компанията следва да има процедура, по която това се извършва, както и да е проведено обучение на служителите и да има документ - вътрешен формуляр, доказващ, че процедурата се контролира и спазва

- Подсилени права на субектите на данни – субектите на данни имат право да знаят какви данни обработвате за тях, как ги обработвате, с кого ги споделяте. Също така имат право да поискат от Вас да изтриете техните данни или да поискат да не ги обработвате за известен период от време (само да ги съхраните, без да ги изтриете). Тези права обаче, не са абсолютни. От значение е правното основание,

на което се обработват данните – дали това е съгласие, договор, легитимен интерес, закон и др.

- Задължение на администратора и обработващия да се грижи за сигурността на данните
- Задължения за обработващите лични данни – не само за администратори
- Задължения за уведомяване на надзорния орган в случай на пробив в системата
- Назначаване на длъжностно лице по защита на личнте данни – в определени случай е задължително

5. Какво включва предложението?

Предложението включва комплекс от дейности, чрез които:

- ✓ се извършва **оценка на текущото състояние** на компанията,т. е. доколко текущото състояние, свързано с обработването на личните данни, съответства на новия Регламент.

Областите, които бъдат идентифицирани като несъответстващи на закона се маркират и съответно клиентът получава препоръки какво да предприеме, за да отстрани слабостите. *Можете да отправите искане към Палатата на и-мейл gdpr@bcci.bg за предоставяне на мостри на оценката.*

- ✓ Препоръките се групират по съответните области, като ги оформяме в отделен документ **„План за действие“**.

Можете да отправите искане към Палатата на и-мейл gdpr@bcci.bg за предоставяне на план за действие.

Допълнително, на база получената информация, ще предоставим:

- ✓ **Становище** дали конкретната компания е длъжна да наеме служител за защита на личните данни
- ✓ Пакет от **образци** на политики и процедури. *Можете да отправите искане към Палатата на и-мейл gdpr@bcci.bg за предоставяне на повече информация.*
- ✓ **Актуализация** в едногодишен срок на политиките/процедурите, формулярите при промени в законодателството или нови добри практики
- ✓ Компютърен **тест за сигурността** на компютърната мрежа. *Можете да отправите искане към Палатата на и-мейл gdpr@bcci.bg за предоставяне на примерен компютърен тест.*

6. Какъв е процесът, по който се извършва услугата?

- След като конкретният клиент сключи договор с Палатата и извърши плащане на услугата, Асоциацията за защита на личните данни изпраща на клиента чрез имейл линк с въпросник и при необходимост осъществява контакт за изясняване на допълнителни въпроси.
- В срок до 20 работни дни от получаване на изцяло попълнения от клиента въпросник Асоциацията за защита на личните данни ще се свърже с клиента и изпрати на посочен от него и-мейл линк с индивидуален достъп до изработените документи.

7. Как се извършва услугата?

Услугата се извършва дистанционно. За целта се използват специализирани въпросници. За целите на компютърните тестове се използват предоставяните от клиента IP адреси (вътрешни и външни, в зависимост от предложението).

8. Какво представляват въпросниците?

Въпросниците са изработени от екип от специализирани експерти в защитата на личните данни. Експертната работна група се състои от юристи, специалисти по информационна сигурност и експерти по внедряване в компании и управление на програма за защита на личните данни.

9. Колко дълги са въпросниците?

Дължината на въпросника зависи от конкретното предложение/специфика на клиента. Най-краткият въпросник се състои от 65 въпроса, а най-дългият е от около 150 въпроса.

10. Има ли определено време за попълване на въпросника?

Въпросникът може да бъде попълнен на етапи, т.е. отговаряте на колкото въпроси прецените днес, запазвате информацията и на следващия ден – продължавате.
При попълнени всички отговори на въпросите – натискате бутон „изпрати“ в края на въпросника. При необходимост, ще бъде поискано предоставянето на допълнителни данни.

11. Как да разбера, че изпратеният от мен въпросник е получен от Асоциация за защита на личните данни?

Асоциация за защита на личните данни ще Ви изпрати кратък и-мейл в рамките на 24 часа с потвърждение за получен попълнен въпросник. В случай че по някаква техническа причина не получите подобно потвърждение, моля да се свържете с представител на Палатата, за да направим допълнителна проверка.

12. Какво е компютърен тест за сигурността на данните?

Компютърният тест е проверка дали данните са достъпни и видими отвън и отвътре, как е защитена мрежата на една фирма, как са защитени хранилищата на данни и трансферът им.

13. Как се извършват компютърните тестове?

Компютърните тестове се извършват дистанционно, като от страна на клиента се изисква информация за IP адреси. В самия въпросник има разяснения как да бъде намерена необходимата информация.

14. Какво представляват включените в услугата компютърни тестове?**

Компютърните тестове са два вида, според избраната оферта (Приложение 1 до 4):
Първият вид е **Външно сканиране** и/или сканиране на сайт
Целта на теста е да се провери доколко външната връзка на клиента е сигурна.
Например, на конкретен сайт на клиента има контактна форма с искане за попълване на лични данни на клиенти. Чрез това сканиране се прави проверка дали има риск тези

данни да бъдат достъпвани от неоторизирани лица и съответно ако има такъв случай, в края на техническия доклад се дават препоръки за отстраняване на откритата слабост.
Вторият вид тест е **Вътрешно сканиране**.
Той показва състоянието на сигурността на данните на ниво единичен запис и служи за обследване на вътрешната ИТ среда.
Във въпросника са дадени инструкции как да бъде намерено конкретното вътрешно IP. Също така, във въпросника са дадени насоки кои компютри е подходящо и трябва да бъдат включени в компютърния тест – това най-общо казано са компютрите, на които се намират основните (чувствителни или по-голямата част) лични данни – например вътрешно IP на компютър на мениджър „Човешки ресурси“, компютър на мениджър „Връзки и обслужване на клиенти“ и т.н.).
Можете да отправите искане към Палатата на и-мейл gdpr@bcci.bg за предоставяне на примерен компютърен тест.

15. Как да съм сигурен в качеството на компютърния тест?

Vulnerability scan и Penetration test са тестове, които са обявени за най-добра практика по всички стандарти за сигурност на информацията и защитата на данни – ISO, PCI DSS, HIPAA.
Тестът се извършва със специални скенери (лицензирани софтуери), по стандарта за сигурност и защита на картовите плащания PCI DSS и се прилага при одитиране на банки и платежни институции. Инструментите в теста - последните данни за уязвимости, вируси и зловредни атаки, се актуализират регулярно на база световно признати стандарти, сред които ISO, SANS Institute, NIST.

16. Какво е различното между 4-те предложения?

Предложенията са адаптирани, като са съобразени спецификите на самите организации:
- Въпросниците за 4-те предложения са различни, за по-големите компании се изисква повече информация, с оглед на това нашите експерти да придобият представа за всичките вътрешните процеси (в общия случаи компании с повече служители и/или отдели имат и повече вътрешни бизнес процеси, свързани със събирането и обработването на данните).
- Компютърните тестове са различни като обхват. В по-малките компании се сканира едно външно IP (колкото имат този тип компании в масовия случай). Като предвид спецификата за не толкова сложна вътрешна мрежа, извършването на вътрешно сканиране не е необходимо на първия етап. В случай че при такъв тип компания след анализа на получената информация, преценим, че има необходимост и от вътрешно изследване на мрежата (например ако открием голям обем чувствителни данни или др.), ще се свършем с клиента допълнително с информация.

17. Какво представлява пакетът от образци на документи (политики/процедури) който ще получа?

Това са изработените от експертите на Асоциацията за защита на лични данни образци на политики, процедури, формуляри, бланки в зависимост от идентифицираните конкретни нужди на даден клиент.

18. Мога ли да съм сигурен, че след като получа Вашите услуги, съм покрил условията на Закона и компанията ми вече оперира в съответствие с него?

Обръщаме внимание, че предоставените от нас услуги включват оценки, препоръки, документация, компютърни тестове. **Планът за действие трябва да бъде имплементиран и спазван от конкретния клиент.**

Допълнително, важно е да се знае, че съответствието със закона е процес. В случай, че клиент, закупил нашата услуга, не предприеме последващи стъпки, например за въвеждането на процедурите и политиките в ежедневието на компанията, не упражни контрол по тяхното спазване, предоставеният от нас пакет няма да му е полезен дългосрочно. На първо време, предоставената оценка и документация биха могли да му служат като доказателство за сериозно отношение към закона, в случай на проверка. За стабилност и дългосрочно решаване на въпроса, необходимо е да се въведат и спазват препоръчаните мерки.

19. Какво от това, че имам оценка и документи, план за действие, като не знам как да го осъществя?

Ако случаят е такъв, клиентът би могъл да се запише в специално предвиденият за целта разяснителен семинар с фокус „имплементация на плана за действие“.

*__Комплексни услуги__ – услуги, свързани с подпомагане въвеждането на изискванията на новия Регламент за защита на личните данни.

**Допълнителна информация относно естеството на компютърните тестове.

Разликата между външен и вътрешен Vulnerability scan:

- Външното автоматично сканиране изследва дистанционно пробивите през външните IP на фирмата – това са IP, които са видими публично и всеки може да ги атакува. Сканират се портовете (външните входове към мрежата на фирмата) и услугите (обменът на информация през тези входове). Подходящо е за фирми с малко компютри или малък обем на съхраняваните и трансферираните данни.

- Вътрешното сканиране изследва вътрешните IP в мрежата на фирмата, които не са видими публично. Това сканиране открива уязвимости на ниво отделен компютър – дали данните в него са защитени от нерегламентиран достъп отвън и отвътре. Например има ли потребителско име и парола, критирани ли са дисковете на компютрите с данни, има ли нива на достъп до данните. Подходящо е за фирми с повече компютри, но и умни устройства, свързани с интернет. Извършва се на място във фирмата или чрез специално изградени тунели за достъп до вътрешната мрежа.

- И двата вида сканиране изследват слабости още на микро ниво, например дали операционната система във фирмата е актуализирана, т.е. защитена от известните към момента пробиви. Както и състоянието на приложените защити и дали са достатъчни - firewall, пароли на рутерите, защити на локалната мрежа и т.н.

Разликата между Vulnerability scan и Penetration test:

- Penetration test включва всичко от двата вида автоматичен Vulnerability scan, но надгражда с ръчно тестване на уязвимостите и точен отчет колко са опасни откритите слабости и какви конкретни щети могат да бъдат нанесени на фирмата. Например Vulnerability scan открива потенциално слаба парола, с Penetration test се прави опит тази парола да бъде разбита. Тестът е симулирана хакерска атака и използва всички инструменти и методи, които биха приложили дигиталните престъпници. След такъв тест компанията има гаранция, че всички известни към момента опасности са експлоатирани и отстранени.