GAP анализ – какво трябва да знае бизнесът за него?

От 25 май тази година всички дейности, свързани с обработване и съхраняване на лични данни във всяка организация подлежат на нова регулация – GDPR. Тя установява много по-стриктни изисквания за защита на личните данни, като една от основните промени е размерът на санкциите. Компаниите е нужно да предприемат редица мерки и то преди обявената дата, за да се подготвят за изискванията на новия режим и да приведат в съответствие с Регламента своите бизнес процеси. Основна стъпка в тази подготовка е установяване на несъответствията между текущото състояние на организацията спрямо изискванията на GDPR или извършване на т.нар. GAP анализ. Какво е GAP анализ и защо е необходим той, разказва доц. д-р Даниела Илиева-Колева, Изпълнителен директор на Фондация „Право и Интернет“ и член на Управителния съвет.

Фондация „Право и Интернет“ е българска неправителствена организация, понастоящем научно-изследователски център. В тази връзка, Фондацията е имплементирала редица международни и национални проекти, в областта на правните, технологичните, икономическите и социалните въпроси, свързани с бързото навлизане на информационните и комуникационни технологии както в публичния, така и в частния сектор, включващи правни анализи и оценка на законодателството, разработване на стратегически документи и анализ на национални политики. Един от основните подходи, използвани от екипа на Фондацията, е именно извършването на GAP анализ. В портфолиото на организацията са както държавни органи, така и частни дружества, доверили се на опита и експертизата на екипа от специалисти, за да получат предварителна оценка и насоки относно привеждането в съответствието на техните системи и процеси със съществуващи или нововъведени стандарти и нормативни изисквания.

1. Първата стъпка към привеждане в съответствие на процесите в дадена организация с нови стандарти и нормативни изисквания, е извършването на вътрешен анализ на работните процеси, известен повече като GAP анализ. Какво би следвало да включва един такъв анализ в контекста на GDPR?

GAP анализът в контекста на GDPR оценява текущото ниво на съответствие с Регламента и помага за идентифицирането и приоритизирането на ключовите области на работа в организацията. Това е един добър начин компаниите да разберат и определят високо рисковите и слабите области на своите процеси по обработване на лични данни, за да са сигурни, че спазват изискванията и не биха понесли така нашумелите огромни по размер глоби. GAP анализът представлява цялостен проект, който стартира с извършването на така наречената „инвентаризация“ на процесите по обработване на лични данни, в рамките на която се идентифицират всички дейности и процеси по обработване на лични данни и техния реален обхват – като например отношенията на компанията с персонала, с контрагенти, клиенти, извършване на дейност по видеонаблюдение и много други. Имайки предвид широкото приложение на GPDR и с оглед постигането на целите на проекта, организацията, която е обект на анализ, следва да осигури участието на всички вътрешни звена. Това би означавало участие в различните етапи на представители на висшия мениджмънт, HR и ИТ отдели, отдел продажби, маркетинг, доставки, логистика (и всички други съответни отдели).

Извършеният GAP анализ дава структуриран поглед върху основните процеси по обработване на лични данни, като отчита рисковете при обработване и включва препоръки за предприемане на конкретни мерки за привеждане или постигане на съответствие с изискванията на нормативната рамка.

2. **След приключване на анализа и получаване на експертно мнение, какво се очаква от администраторите на лични данни и съответно от / обработващите лични данни да предприемат като действия?**

След приключване на GAP анализа, компанията следва да предприеме мерки по привеждане в съответствие с изискванията на GDPR. С оглед спазване на изискванията за прозрачност, документиране и отчетност е необходимо ревизиране, адаптиране и изготвяне на определени вътрешни документи, така че да се обезпечи законосъобразното обработване на лични данни в структурата на съответната организация. Конкретни мерки, които администратори или обработващи лични данни следва да предприемат, са поддържането на детайлни регистри на всички основни дейности по обработване съгласно чл. 30 от Регламента, актуализиране или изготвяне на политика за защита на личните данни и/или поверителност, уреждане на отношенията администратор-администратор, администратор-обработващ чрез договори или анекси към договорите, разработване на процедури за събиране на съгласия от субектите на данни, разработване на процеси за упражняване на правата на физическите лица, и в определени случаи, назначаване на длъжностно лице по защита на данните.

3. Разкажете ни повече за фигурата на „Длъжностно лице по защита на данните“.

Длъжностното лице по защита на данните лежи в основата на новите изисквания на GDPR, и определянето му е задължително в конкретните случаи, предвидени в чл. 37 от Регламента.

Концепцията за Длъжностното лице по защита на данните не е съвсем нова, тъй като това е длъжност, съществуваща до момента в други европейски държави като Германия и припозната като полезна за организациите, с оглед спазването на приложимите изисквания за защита на личните данни. В България и досега е съществувала правна възможност, но не и задължение за назначаване на лице по защита на личните данни.

GDPR обаче въвежда напълно нови функции на Длъжностното лице по защита на данните, което следва да изпълнява широк набор от дейности. В обхвата на длъжността влиза задачата да изпълнява ролята на „точка за контакт“ за надзорния орган, както и за физически лица по въпроси, свързани с обработването на техни лични данни и упражняването на техни права, да информира и съветва администратора за задълженията, да наблюдава текущо спазването на изискванията на Регламента, да докладва директно на ръководството на организацията.

Най-общо това е „отговорникът“ по защита на личните данни, който помага на компаниите да спазват основните изисквания за отчетност, прозрачност и документиране.

4. Регламентът посочва два варианта за определянето му – член на персонала или външна аутсорсинг услуга? Какви фактори трябва да се взимат предвид при взимането на решение за определянето му?

При назначаването му като член на персонала, на първо място, компаниите трябва да имат предвид, че Длъжностното лице по защита на данните е една независима фигура. В тази връзка, за да се осигури неговата независимост както и директно сътрудничество с ръководството на компанията, следва то да бъде назначено на висока йерархична позиция. Особено важен аспект е да се следи за възникването на конфликт на интереси, в случаите на съвместяване на длъжности. Служителят по Човешки ресурси, ИТ служител, вътрешния юрисконсулт или служители на ръководно ниво, директно въвлечени в обработването на лични данни и определящи целите и средствата на обработването, не могат да изпълняват тази длъжност. В повечето случаи в компанията почти няма длъжност, която да не влиза в

този обхват. При наемане на служител, организацията, обаче, следва да осигури и достатъчна степен на натовареност на лицето както и неговата взаимозаменяемост, в случаите на негово отсъствие.

При подбора на длъжностно лице, следва да се вземат предвид не само неговите професионални умения в областта на защита на личните данни, но и неговите познания в индустрията и комуникативните му качества, които ще му помагат ефективно да си сътрудничи с надзорния орган, със субектите на данни и с ръководството на компанията.

В случаите на аутсорсинг на дейността на външен изпълнител, организацията възлага задълженията на Длъжностно лице по защита на лични данни на подготвен екип от експерти, които да изпълняват тази роля. Тази организация се ангажира на база договор за услуги да предоставя качествена услуга, като поема задължение за конфиденциалност и осигурява поемането на такива задължения и от всички участници в екипа й. По този начин се гарантира в по-голяма степен независимост на длъжностното лице, с което намалява и рискът от възникване на конфликт на интереси. Конфликт на интереси в тези случаи би възникнал, ако длъжностното лице бъде поканено да представлява компанията в съдилища по дела, свързани със защитата на личните данни.

5. При евентуално нарушение и налагане на глоба на дадена организация, до каква степен „Длъжностното лице по защита на данните“ носи отговорност?

Първо нека споменем, че администраторът или обработващият носи отговорност за спазване на изискванията на Регламента. Длъжностното лице е това, което чрез своя независим експертен съвет помага на организацията надлежно да прилага тези изисквания и да поддържа едно постоянно високо ниво на защита на личните данни. За да се избегнат подобни ситуации, би било полезно длъжностното лице да бъде в голяма степен въвлечено и ангажирано с голяма част от въпросите по обработване и защита на личните данни, така че своевременно да съветва и информира за потенциални рискове. Длъжностното лице, обаче, не взима и не трябва да взима самите решения, свързани с обработването на данните. То дава независими съвети и насоки, с които администраторът или обработващият могат да се съобразят или не по тяхна преценка.

И все пак, при възникване на ситуация, в която Длъжностното лице не изпълнява, свързаните с функцията му задължения, дейността му може да бъде преустановена или да бъде освободено от длъжност съгласно приложимото договорно или трудово право.

6. Забелязва се, че „ Длъжностно лице по защита на данните? “ се обособи като отделна, чисто нова професия. Какъв съвет бихте дали на компаниите при избора на такова лице?

В момента се очертава интензивно търсене на „Длъжностно лице по защита на данните“. Ако компаниите изпитват трудност да подберат подходящ член на персонала, то както вече споменахме, съществува и възможност за определяне на външен изпълнител. Много компании в България вече предлагат тази услуга като част от разнообразното си портфолио, а други се фокусират в аутсорсинг само на длъжностни лица по защита на данните.

Изборът остава в ръцете на организациите, но определянето на такова лице следва да е добре обмислено и отговорно решение.