7.Защита на личните данни (ЗЛД)

-**Данните са новата валута** [Д-р Вивиан Балакришнан, Министър на външните работи на Сингапур]. **Няма** бизнес, който да може да функционира без да обработва ЛД. **Няма** онлайн услуга, която да можем да използваме без да предоставим личните си данни

Личните данни са може би **най-важният** икон. ресурс на 21-ви век.

Неприкосновеност на личната сфера (privacy): Правото да бъдем оставени сами; **Контрол върху информацията; Нещо лично, концепция за сфера на интимно пространство**

Неприкосновеност личната сфера vs. Защита личните данни: Свързани помежду си – всяко от тях защитава интимната, лична сфера на хората; **Диаметрално противоположни;** Принципът при неприкосновеността на личната сфера е „**забранено е освен ако …**“ (намеса от страна на полицията и т.н.); Принципът в защита на личните данни е „**разрешено е, ако …**“

Развитие защитата личните данни в Европа Се учи слайда

-Насоки относно защитата на личната неприкосновеност и трансграничния поток на ЛД (ОИСР) – 1980 & **Конвенция 108** за защита лицата при автоматизираната обработка ЛД (Съвета на Европа) – 1981 – Отворена за държави не само в Европа

-Хартата на основните права на ЕС (**чл. 8**) – **2000**

-Май 2016 –реформа, включваща следния пакет от актове: **Регламент (ЕС) 2016/679 (GDPR), Директива (ЕС) 2016/680** относно обработването на ЛД от полицейските органи

-Директива (ЕС) 2016/681 относно обработването на резерв. данни на пътници с цел борба срещу тероризма и тежките престъпления

-Регламент 2018/1725 – за обработване на ЛД от институции, органи, служби и агенции на ЕС

Защита на личните данни в България:

- Конституция на Република България (**Чл. 32. (1) Личният живот на гражданите е неприкосновен. Всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име. (2) Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи.**

-Закон за защита на личните данни/Допълва GPTR - не е водещ/

-Правилник за дейността на Комисията за защита на личните данни и на нейната администрация и др.

Основни понятия на защитата на личните данни

ЛД – всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицивано(“субект на данни”); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци специф. за физическата, физиологичната, генетичната, психологическата, умствената, икономическата, културната или социална идентичност на това лице.

данните – **съвкупност от обективни признаци на явление, процес или променлива/лат. факт/** ; **информацията** – **данни в контекст /подредени/**

Обработване на ЛД – всяка дейност, която се извършва с ЛД

Администратор на ЛД – всяко лице, (физическо/юридическо, публичен орган, агенция) което самостоятелно или съвместно с др. **определя целите и средствата за обработването** на ЛД

Обработващ ЛД – всяко лице, (физическо/юридическо, публичен орган, агенция) **което обработва ЛД от името на администратора**

Субект на данни – физическото лице, за което данните се отнасят

Надзорен орган – в Бг е **Комисията за защита на личните данни**; за съдебните дейности – Инспектората към Висшия съдебен съвет

Администратори/работатели/ на личнни данни: **предприятията**, обработващи данните на своите **служители, клиенти и доставчици**;

Обработващи ЛД: доставчици на облачни услуги, услуги по настаняване, доставчици на счет. услуги, IT услуги и др.

!!! Служителите на администратора на ЛД са част от самия администратор, те **не са** обработващи ЛД.

Обща х-ка на GDPR (General Data Protection Regulation):Пряко действие – няма необходимост от транспониране чрез приемане на нормативни актове на национално ниво; Прилага се от **25.05.2018 г.; Еднакво прилагане в рамките на ЕС; Имуществени санкции по Регламента:** Ефективни, пропорционални и възспиращи; „Нарушенията … подлежат … на административно наказание „глоба“ или „имуществена санкция“ в размер **до 20 000 000 EUR ИЛИ, в случай на предприятие — до 4 % от общия му**

годишен световен оборот за предходната финансова година, която от двете суми е по-висока”

Материален обхват(чл. 2, GDPR**)**- Прилага се за обработв. на ЛД;

регистър с ЛД - всеки структуриран набор от ЛД, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

GDPR **Не се прилага за обработване: От ФЛ в хода на чисто лични или домашни занимания;**

Териториален обхват (чл. 3) =

- **Критерий по място на установяване:** Обработване на ЛД в контекста на дейностите на дадено **място на установяване** на администратор/обработващ в ЕС;

-**Таргетиращ критерий**: Обработване на ЛД от администратор/обработващ, който не е установен в ЕС, но обработва ЛД на субекти, намиращи се в ЕС, при: **предлагането на стоки/услуги на субекти на данни в ЕС; или наблюдението на тяхн. поведение**, доколкото е ЕС.

-Обработване на ЛД от администратор, който не е установен в ЕС, но е установен на място, където **се прилага правото на държава членка по силата на международното право** (круизен кораб)

Принципи на защитата на личните данни: Законосъбразност, добросъвестност и прозрачност; Ограничение на целите; Свеждане на данните до минимум; Точност; Ограничение на съхранението; Цялостност и поверителност (мерки за защита); ОТЧЕТНОСТ

Основания за законосъобразно обработване на ЛД:

- има: **правно основание** - **Условие**, предвидено от правото, което, ако е изпълнено, е достатъчно за обработването на ЛД.

- 3 отделни категории лични данни, към които са приложими различен набор правни основания: 1/Данни, които не попадат под специален режим; 2/Данни под специален режим: **а)Спец. категория данни („чувствителни данни“); б)Данни за присъди и нарушения;**

Основания по чл. 6 от Регламента: 1/**Съгласие; 2/Договор със субекта на данните; 3/Законово задължение; 4/Жизненоважни интереси; 5/Обществен интерес; 6/ Легитимен интерес**

Обработване на чувствителни данни/интимни данни/

Логика за опред. категория данни като чувствителни: Контекстът на тяхната обработка би могъл да създаде значителни рискове за основните права и свободи на гражданите и засяга много интимни области от техния живот; Обработването на тези данни **е забранено** и могат да бъдат обработвани само при изключителни обстоятелства; Различните видове данни имат различно въздействие върху отделните хора (т.е. **обективен подход** при дефинирането им, силно повлиян от антидискриминационното законодателство); Принципът е подобен на неприкосновеността на личния живот “**забранено е**, освен ако….”

Конкретните категории: ЛД, разкриващи расов или етнически произход; политически възгледи, религиозни, философски убеждения, членство в синдик.орг-ции; генетични данни, обработване на биометрични данни за целите единствено на идентифицирането на физическо, данни за здравословното състояние , данни за сексуалния живот или сексуалната ориентация

Условия за обработване на чувствителни данни: Изрично съгласие; Права/задълж. в трудовото, осигурителното право, социалната закрила (предвидено в правото на ЕС/ държава членка или в КТД - колективен трудов договор); Жизненоважни интереси, ако не може да се получи съгласие; Обработване в рамките ЮЛНЦ - Юридически лица с нестопанска цел; Субектът е направил данните обществено достояние; Правни претенции; Важен обществен интерес; Медицина; Обществен интерес в областта на общественото здраве; Архивиране в обществен интерес, за научни/ исторически изследвания или за статистически цели

Обработване на данни за присъди и нарушения: НЕ са специални категория данни; специален режим за обработването им

Обработването се осъществява **п**ри наличието едно от следните две **допълнителни** условия:

-Обработването се извършва под контрола на официален орган

-Обработването е разрешено от правото на ЕС/на държава членка;

Разширен набор права на субектите на данни: Право на информация – прозрачност; Право на достъп; Право на коригиране; Право на изтриване ("право да бъдеш забравен"); Право на ограничаване на обработването; Задължение за уведомяване при коригиране или изтриване на ЛД или ограничав. на обработването; Право на преносимост на данните; Право на възражение; Право да не бъде обект на автоматизирано вземане на индивидуални решения, вкл. профилиране

Право на информация - Съществува още по ЗЗЛД преди приемането на GDPR: данни за администратора/ неговия представител; целите на обработването на личните данни;

получателите или категориите получатели; данните за задължителния; информация за правата; категориите ЛД;

Допълнителни изисквания по GDPR: Координати за връзка с длъжностното лице по защита на данните; Целите и **правното основание** за обработването; При основание законен интерес – конкр. законен интерес; Трансфери на данни извън ЕС; Срок за съхранение на данните/ критерии за определянето му; Право на оттегляне на съгласието и другите нови права по ОРЗД- Общ регламент относно защитата на данните (преносимост, възражение); Право на жалба до надзорен орган; Информ. за автоматизирано вземане на решения/ профилиране

Отношения администратор-обработващ

Нормативни задължения и отговорност за обработващите ЛД:

Договор между администратора и обработващия; Обработват данните само по документирано нареждане на администратора; Информират незабавно администратора, ако считат че нареждането му нарушава действащата уредба; **Поддържат регистър на всички категории дейности по обработването, извършени от името на администратор**

Съвместни администратори: Нова фигура, въведена с чл. 26 ОРЗД; Двама или повече администратори, които съвместно определят целите и средствата на обработването; **Задължения – договореност,** с която да определят **по прозрачен начин** съответ. си отговорности

Независими администратори: уреждането на отношенията по обмена на данни с **договор**;

Задължения на администратора и обработващия ЛД: Защита на данните на етапа на проектир. и по подразбиране (privacy by

default & privacy by design)**; Водене на регистри; Оценка на въздействието; ДЛЗЛД; Сътрудничество с надзорния орган; Сигурност на личните данни;**

Защита на данните по проектиране – всеки нов бизнес трябва да вземе под внимание защитата на личните данни. Задължение да се приемат подходящи технически и организационни мерки

Защита на ЛД по подразбиране – автоматично да се приложат най-стриктните условия за защита на ЛД след като клиентът е придобил нов продукт. **Само** ЛД **необходими** за съотв. цел да се обработват

Водене на регистри:

-**Субект на задължението**: администратори **И** обработващи

-**Същност**: документиране на дейностите по обработване на ЛД

-**Цел**: намаляване на административната тежест за бизнеса

-Праг от **250 служители,** но такива регистри трябва да се поддържат във всяко предприятие.

Нарушение на сигурността: Подходящи техн. и организационни мерки; Уведомение при нарушаване сигурността на ЛД; Съобщаване за нарушаване на сигурността на личните данни

Оценка на въздействието:

-**Предпоставки**: при вероятност определен вид обработване да породи висок риск за правата и свободите на физическите лица

-**Задължителна при**: Автомат. вземане на решения/ профилиране; Мащабно обработване на спец. категории ЛД /присъди и нарушения/; Системат.мащабно наблюдение публич. достъпна зона

-**Предварително** – преди започване на обработването

-Роля на КЗЛД(**Комисия за защита на личните данни**): Предварителна консултация (при висок риск); Списък на видовете операции по обработване, за които се изисква (**задължителен**)/ не се изисква оценка на въздействието (**пожелателен**)

ДЛЗЛД- Задължително, ако администраторът/обработващ. ЛД е:

-публичен орган/структура (с изкл. на съдилища), или

-Основните дейности се състоят в: редовно и систематично мащабно наблюдение на субектите на ЛД; мащабно обработване на спец. категории данни и на данни, свързани с присъди и нарушения

-Държавите членки/ЕС може да предвидят и др. случаи, когато ДЛЗЛД трябва задължително да бъде назначено.

ДЛЗЛД: Участва във **всички въпроси** по защитата на ЛД; Трудов договор; Договор за услуги; Единна точка за контакт; **Независимост**

Трансфер на ЛД: 1/Свободно в ЕС/ЕИП; 2/При предаване на трети страни/межд. организации, трябва да се осигури **адекватно ниво на защита**: а)Решение на Европейската комисия (**списък**); б)При липса на решение – подходящи гаранции – с или без разрешение от надзорните органи (КЗЛД): Стандартни договорни клаузи за защита на ЛД, Задълж. фирмени правила, Дерогации по чл. 49 GDPR и др

Надзорен орган и ЕКЗД(Европейск.комитет по защита на данните**):**

-Всяка държава членка осигурява един или повече независими публични органи, които са отговорни за наблюдението на прилагането на GDPR, за да се защитят осн. права и свободи на физич. лица във връзка с обработването и да се улесни свободното движение на ЛД в рамките на ЕС („**надзорен орган**“)

-Компетентност и водещ надзорен орган при трансгранично обработване на данни

Право на жалба § съдебна защита: Жалба до надзорен орган; Право ефективна съдебна защита срещу надзорен орган; Право на ефективна съдебна защита срещу АЛД

Особени нац. правила:

Необходимост: Синхронизиране с GDPR – административни въпроси + премахване на текстове, противоречащи на Регламента; Нац. правила, приети в рамките на позволеното от Регламента;

-Обучения от КЗЛД

-Общи правила и особени случаи на обработване на ЛД

-Професионална тайна на администратора/обработващия

-Упражняване и ограничаване на права

-Срокове за жалба до КЗЛД (6 месеца от узнаването на нарушението, но не по-късно от 2 години от извършването му);

-Национални санкции

Обработване на ЛД за полицейски дейности:

-Извън приложното поле на GDPR, се прилага Директива 2016/680, транспонирани в глава 8 ЗЗЛД

-Компетентни органи = държавните органи, които имат правомощия по предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи

-Администратор = компетентен орган/ административна структура, част от която е този орган, които самостоятелно или съвместно с други органи определят целите и средствата за обработване на ЛД