7.Защита на личните данни (ЛД)

Защо защита на личните данни?

-**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** икономически ресурс на 21-ви век. Оттам и опазването им е ключова стратегическа цел за всяка държава и частна организация

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 …“ (например намеса от страна на полицията и т.н.)
- Принципът в защита на личните данни е „разрешено е, ако …“ (ако всички изисквания в закона за защита на личните данни са съобразени– правно основание за обработка+ цели + правата

субектите, чиито данни се обработват/ задължения администратора са съобразени – позволено обработване ЛД)

Развитие защитата личните данни в Европа **Се учи слайда**

- Всеобща декларация за правата на човека на ООН 1948 & Европейска Конвенция за правата на човека – 1950: право за зачитане на личния и семейния живот
- Закон за защита на личните данни на Хесен, Германия – 1970
- Немски федерален закон за защита на личните данни – 1977
- 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
- Директива 95/46/ЕС
- Хартата на основните права на ЕС (**чл. 8**) – 2000
- Договор за функционирането на Европейския съюз – 2007 (Лисабон): Чл. 16: всеки има право на защита на личните му данни
- Май 2016 –реформа, включваща следния пакет от актове:
- **Регламент (ЕС) 2016/679 (GDPR)**
- **Директива (ЕС) 2016/680** относно обработването на ЛД от полицейските органи (транспонирани в глава осма ЗЗЛД)
- Директива (ЕС) 2016/681 относно обработването на резервационни данни на пътници с цел борба срещу тероризма и тежките престъпления (транспонирана в ЗДАНС)
- 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 – изменен през фев. 2019 г./2023 г./Допълва само GPTR - не е водещ/

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

- Специални нормативни актове – ЗМВР, ЗЗдр, ЗКИ, ЗЕС 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 специфични за физическата, физиологичната, генетичната, психологическата, умствената, икономическата, културната или социална идентичност на това лице.

- Какво са **данните**? – **съвкупност от обективни признаци на явление, процес или променлива/лат. факт/**

Пример: 180, 4222443, 8804162256, син, тъмен, висок, Иванов, български, румънски, Иван, Ива, 41 24 12.2 N 2 10 26.5 E

- Какво е **информацията**? – **данни в контекст /подредени/**

- **Обработване на ЛД – всяка дейност, която би могла да се извършва с ЛД** (включително съхранение, трансфериране, изтриване или модификация)

- **Администратор на ЛД** – всяко лице, (физическо/юридическо, публичен орган, агенция или друга структура) което самостоятелно или съвместно с други **определя целите и средствата за обработването** на ЛД/data controller/

- **Обработващ** ЛД – всяко лице, (физическо/юридическо, публичен орган, агенция или друга структура) **което обработва ЛД от името на администратора**/administrator може да outsorse/

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

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

Примери

Администратори/работатели/ на личнни данни са: предприятията, когато обработват данните на своите служители, данните на своите клиенти и доставчици; държавните органи, при упражняването на техните правни задължения

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

NB! 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
- Все пак е необходимо съобразяване на изискванията му в националното законодателство
- В сила – 20 дни след публикуването му на 04.05.2016 г.
- 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”**

- Приложно поле

 Материален обхват (чл. 2) = Прилага се за обработването на ЛД

 изцяло или частично с автоматични средства, както и

 с други средства, като личните данни са част от регистър с ЛД или са предназначени да съставляват част от такъв

- **„регистър с ЛД“ означава 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; (чл. 4, т. 6 GDPR)**

Не се прилага за обработване:

- в хода на дейности, които са извън приложното поле на правото на ЕС (напр. отбрана и национална сигурност)
- от държавите членки, когато извършват дейности, които попадат в приложното поле на дял V, глава 2 от ДЕС (външна политика и политика за сигурност на ЕС)
- **От ФЛ в хода на чисто лични или домашни занимания**
- от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност
- Обработване от от институциите, органите, службите и агенциите на ЕС
- **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, независимо дали обработването се извършва в ЕС или не;
- **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, независимо дали се изисква плащане; или

 наблюдението на тяхното поведение, доколкото то се проявява в рамките на 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, дипломатическо/консулско представителско)

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

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

Различаваме 3 отделни категории лични данни, към които са приложими различен набор правни основания:

- Данни, които не попадат под специален режим – основанията за тях са в чл. 6, пар. 1 GDPR

- Данни под специален режим, които биват:

- **Спец. категория данни („чувствителни данни“) – условието за тяхното обработване е разписано в чл. 9, пар. 2 GDPR**

- **Данни за присъди и нарушения – специалните правила за тяхното обработване са уредени в чл. 10 GDPR**

Основания по чл. 6 от Регламента:

- **Съгласие**
- **Договор със субекта на данните / преддоговорни стъпки**
- **Законово задължение**
- **Жизненоважни интереси**
- **Обществен интерес / официални правомощия**
- **Легитимен интерес**

Обработване на чувствителни данни/интимни данни/

- Логика зад закрепването на определена 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, изчерпателно изброени в законодателството за защита на данните на ЕС и държавите членки;
  - ✓ 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…."

Обработване на чувствителни данни

- Конкретните категории са изброени в чл. 9, пар. 1 GDPR:

✓ ЛД, разкриващи расов или етнически произход,
✓ политически възгледи,
✓ религиозни или философски убеждения или членство в синдикални организации,
✓ генетични данни,
✓ обработване на биометрични данни за целите единствено на идентифицирането на физическо лице (N.B.! Внимание с ползването на камери за лицево разпознаване),
✓ данни за здравословното състояние (N.B.! Повишено внимание при обработването на такива данни в условията на пандемия в стремежа да се въведат противоепидемични мерки на работното място)
✓ данни за сексуалния живот или сексуалната ориентация на физическото лице.

Условия за обработване на чувствителни данни

- Изрично съгласие
- Права/ задължения 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 (за настоящи/ бивши членове или контакти)
- Субектът е направил данните обществено достояние

- Правни претенции/ съдебни органи при правораздаване
- Важен обществен интерес – в правото на ЕС/ държава членка
- Медицина (трудова, превантивна, диагностика и т.н.)
- Обществен интерес в областта на общественото здраве (борба със заплахи за здравето, безопасност на лекарствата и т.н.)
- Архивиране в обществен интерес, за научни/ исторически изследвания или за статистически цели

Обработване на данни за присъди и нарушения

- НЕ са специални категория данни
- Чл. 10 GDPR урежда специален режим за обработването им/свидетелство за садимост се изиска за преподавател, счетоводител/

o Обработването се осъществява **въз основа чл. 6, пар. 1 GDPR**

o При 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 (разширено) – Принцип на прозрачност

 Право на достъп (разширено)

 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 ограничаване на обработването**
- **Право на преносимост на данните**
- **Право на възражение**
- **Право да не бъде обект на автоматизирано вземане на индивидуални решения, включително 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/ доброволния х-р на предоставяне на данните и последиците от отказ за предоставянето им;
  - информация за правата
  - категориите ЛД (ако не се събират пряко от субекта)
- Допълнителни изисквания по GDPR
  - Координати за връзка с длъжностното лице по защита на данните
  - Целите и **правното основание** за обработването
  - При основание законен интерес – конкретния 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
- Информация за автоматизирано вземане на решения/ профилиране

Отношения администратор-обработващ

Нормативни задължения и отговорност за обработващите ЛД

- Договор между администратора и обработващия (писмен – чл. 28 GDPR)
- Превъзлагане на дейностите по обработване само след предварително писмено конкретно или общо съгласие/ одобрение от администратора
- Информират администратора за всяка планирана промяна в превъзлагането
- Обработват данните само по документирано нареждане на администратора
- Ангажименти за конфиденциалност за персонала им
- Информират незабавно администратора, ако считат че нареждането му нарушава действащата уредба
- **Поддържат регистър на всички категории дейности по обработването, извършени от името на администратор**

Отношения администратор-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** съответните си отговорности (освен ако отговорностите не са определени в правото на ЕС/държава членка), по-специално:

- упражняване на правата на субекта на данни

- информираност по чл. 13 и 14 ОРЗД

- може да се посочи точка за контакт за субектите на данни

- **Независими администратори**

- Силно препоръчително е уреждането на отношенията по повод обмена на данни с **договор** (арг. от принципа за отчетност)

- Примерно съдържание: категории данни; субекти; цели; основания; срок на обработването; гаранции (вкл. мерки за сигурност); задължения за сътрудничество

Задължения на администратора и обработващия ЛД

- **Защита на данните на етапа на проектирането и по подразбиране (privacy by default & privacy by design)**
- **Водене на регистри**
- **Оценка на въздействието**
- **Длъжностно лице по защита на данните**
- **Сътрудничество с надзорния орган**
- **Сигурност на личните данни (допълнителни изисквания)**

Защита данните на етапа на проектирането и по подразбиране

- **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 данните по подразбиране** – автоматично (по подразбиране) да се приложи най-стриктните условия за защита на личните данни след като клиентът е придобил нов продукт/услуга. **Само** ЛД **необходими** за съответната цел трябва да бъдат обработвани.

Водене на регистри

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

- **Същност**: надлежно документиране на дейностите по обработване на личните данни в писмена (включително и електронна) форма

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

- **Последици**: от 25.05.2018 задължението на администраторите за

регистрация в КЗЛД вече не се прилага.

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

Нарушение на сигурността

- **Подходящи технически и организационни мерки**

- Нивото на сигурност трябва да е адекватно на нивото на риск

- **Уведомение при нарушаване сигурността на личните данни**

 Към надзорния орган (без ненужно забавяне, не по-късно от 72 часа след узнаване за нарушението на сигурността);

 От обработващия към администратора (без ненужно забавяне след узнаване за нарушението)

- **Съобщаване за нарушаване на сигурността на личните данни** към субекта на личните данни, ако нарушението може да доведе до висок риск за правата и свободите на физическото лице

Оценка на въздействието

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

 Автоматизирано вземане на решения/ профилиране

 Мащабно обработване на специални категории данни/ данни за присъди и нарушения

 Систематично мащабно наблюдение публично достъпна зона

- **Предварително** – преди започване на обработването
- Минимално изискуемо съдържание на оценката (писмено)
- Роля на КЗЛД

 Предварителна консултация (при висок риск)

 Списък на видовете операции по обработване, за които се изисква (задължителен)/ не се изисква оценка на въздействието (пожелателен)

Длъжностно лице по защита на данните

Задължително, ако администраторът/обработващият ЛД:

- е публичен орган/структура (с изключение на съдилища при изпълнение

на служебните им функции), или

- Основните дейности се състоят в:

-редовно и систематично мащабно наблюдение на субектите на ЛД

-мащабно обработване на специалните категории данни и на данни, свързани с присъди и нарушения

- **Държавите членки/ЕС може да предвидят и други случаи, когато длъжностно лице по защита на данните трябва задължително да бъде назначено.**
- Участва във **всички въпроси** по защитата на личните данни
- Трудов договор (конфликт на интереси!)
- Договор за услуги
- Единна точка за контакт
- **Независимост**

Трансфер на ЛД

- **Свободно в ЕС/ЕИП**
- При предаване на трети страни/международни организации, трябва да се осигури **адекватно ниво на защита**:

 Решение на Европейската комисия (списък)

 При липса на решение – подходящи гаранции – с или без разрешение от надзорните органи (КЗЛД):

 Стандартни договорни клаузи за защита на данните (?)

 Задължителни фирмени правила

 Дерогации по чл. 49 GDPR

- Други инструменти

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 личните данни в рамките на ЕС („**надзорен орган**“)
- Независимост (чл. 52), задачи (чл. 57) и правомощия (чл. 58)
- **Компетентност (чл. 55) и водещ надзорен орган при трансгранично обработване на данни** (чл. 56)
- Сътрудничество (чл. 60), взаимопомощ (чл. 61), съвместни операции (чл. 62), съгласуваност (чл. 63)
- ЕКЗД (чл. 68-76)

Право на жалба § съдебна защита

- **Жалба до надзорен орган** (чл. 77)
- по обичайно местопребиваване
- по място на работа
- по място на предполагаемото нарушение
- задължение на надзорния орган за информиране на жалбоподателя за напредъка в разглеждането на жалбата и за резултата от нея, включително за възможността за съдебна защита

• Право ефективна съдебна защита срещу надзорен орган (чл. 78)

- по място на установяване на надзорния орган

- **Право на ефективна съдебна защита срещу АЛД/обработващ (чл. 79)**

 по място на установяване на АЛД/обработващия

 по обичайно местопребиваване, освен ако АЛД/обработващият е публичен орган на държава членка, действащ в изпълнение на публичните си правомощия

Особени национални правила

- **Измененията са факт от 26.02.2019 г., в сила от 02.03.2019 г.**
- **Необходимост**

 Синхронизиране с GDPR – административни въпроси + премахване на текстове, противоречащи на Регламента

 Нац. правила, приети в рамките на позволеното от Регламента

 Транспониране на Директива 2016/680

- **Обучения от КЗЛД**
- **Общи правила и особени случаи на обработване на ЛД (чл. 25а-25о ЗЗЛД)**

 Предоставяне на ЛД без правно основание/ в противоречие с принципите

 Уведомяването на КЗЛД за назначаването на ДЛЗД

 Съгласие на деца

 Копиране на документ за самоличност

 Правила при мащабно обработване на ЛД или при систематично мащабно наблюдение на публично достъпни зони, включително чрез видеонаблюдение

 Спец. правила за обработване на ЛД на починали лица

 Обработване на ЕГН

 Обработване на лични данни за журналистически цели, за академичното, художественото, литератур. изразяване

 Особени правила в трудовото право

 Вътрешни правила и процедури при (1) използване на система за докладване на нарушения (2) ограничения при използване на вътрешнофирмени ресурси; (3) въвеждане на системи за контрол на достъпа, работното време и трудовата дисциплина

 Срокове за съхранение на данни при подбор на персонал

 Обработване ЛД за целите на Нац. архивен фонд

 Обработване за научни/исторически/статистически цели

 Обработване за хуманитарни цели

- **Професионална тайна на администратора/обработващия**
- **Упражняване и ограничаване на права**

Начини (чл. 37б ЗЗЛД):

 Чрез писмено заявление до администратора или по друг определен от администратора начин

 По електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ), ЗЕУ и Закона за електронната идентификация

 Чрез действия в потребителския интерфейс на информационната система, която обработва данните

Реквизити (чл. 37в ЗЗЛД)

- **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, прилагат се правилата на 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 за обществената сигурност и тяхното предотвратяване (чл. 42, ал. 4 ЗЗЛД)
- **Администратор** = компетентен орган или съответната административна структура, част от която е този орган, които самостоятелно или съвместно с други органи определят целите и средствата за обработване на ЛД (освен ако закон предвижда друго).
- В Закона съдебната власт липсва конкретна норма кой е администратор, така че би следвало това да са съответните ЮЛ (съд, прокуратура и т.н.)
- Особености при принципите, правните основания, обхват и упражняване на правата