ОБЩ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ 2016/679

ЦАНКО ЦОЛОВ

Член на Комисията за Защита на Личните Данни

ЗА РЕГЛАМЕНТА

- Публикуван на 4 май 2016г. Влиза в сила от 4 май 2018г.;
- Има пряко действие;
- Модернизиране на правила за защита на личните данни с оглед на бързото развитие на технологиите и глобализацията;
- Увеличаване доверието на потребителите в онлайн услугите;
- Хармонизиране правилата целия ЕС;
- Да се даде на лицата по-голям контрол върху данните им в дигиталния свят;
- По малка бюрократичната тежест за бизнеса.

ЦЕЛИ НА РЕГАЛМЕНТА

ЗАЩИТА ПРАВАТА И ЛИЧНИТЕ ДАННИ НА ГРАЖДАНИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Контрол от страна на субектите

ОСИГУРЯВАНЕ НА СВОБОДЕН ОБМЕН НА ДАННИ

Единен цифров пазар

МОДЕРНИЗАЦИЯ НА ЗАКОНОДАТЕЛСТВОТО

Нови технологии

КЛЮЧОВИ ПРОМЕНИ

- Обработването ще породи висок риск;
- оценка на личните аспекти, базирана на автоматично обработване, включително профилиране, и служи за основа на решения;
- мащабно обработване на специални категории данни;
- мащабно наблюдение на публична зона.

- Необходимостта от демонстриране на съответствие с принципите законосъобразност, справедливост и прозрачност, ограничаване на целите, минимизиране на данните, точност и ограничаване на съхранението

- В публичен орган;
- мащабно наблюдение на субектите на данни;
- мащабно обработване на специалните категории данни .

- Приетите мерки съответстват на риска
- До 72ч трябва да се уведомят надзорния орган и засегнатите лица

- Изтриване, достъп, коригиране, възражение, ограничение и преносимост
- Достъп до данните по лесен и разбираем начин

- Обработването е законосъобразно при: съгласие, необходимост, правно задължение, защита, публичен или законен интерес или официална власт;
- Съгласието - дадено свободно, специфично, информирано, недвусмислено и изрично;
- Не е законосъбразно съгласие по подразбиране.

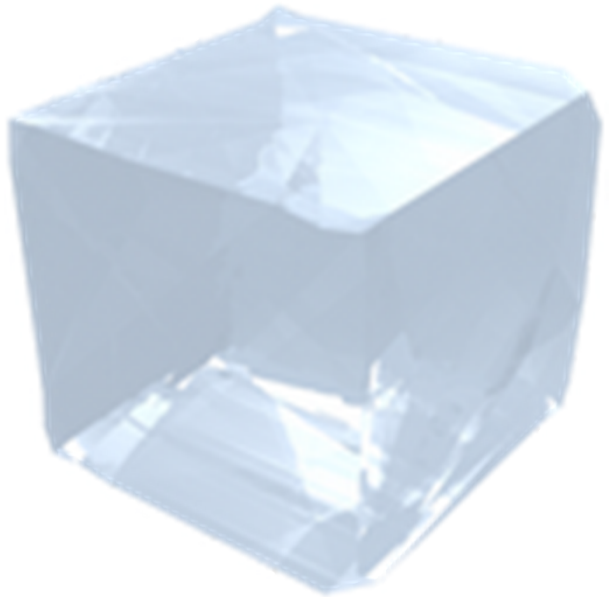
- Неприкосновеност при изграждане на системите privacy by design, privacy by default;
- Всички искания за съгласие са по подразбиране “не”

КОМПАНИЯТА през ПОГЛЕДА на GDPR

ОТЧЕТНОСТ

Задължението на дадено лице или организация да отчита дейността си, да поема отговорност и да оповестява резултатите по прозрачен начин.

- Управленска структура;
- Преглед на личните данни;
- Политики за неприкосновеност на данните;
- Прилагане на защитата при обработката;
- Програма за обучение;
- Управление на риска за информационната сигурност;
- Управление на риска от трети страни;
- Уведомления при пробив в системата;
- Поддържане процедури за запитвания и жалби;
- Мониторинг за нови оперативни практики;
- Програма за управление на нарушенията;
- Мониторинг на процедурите за обработване;
- Следене на външните критерии



УПРАВЛЕНСКА СТРУКТУРА

наличие на лица, отговорни за защитата на личните данни и процедури за управление на отчетността

- **Провеждане на оценка риска за неприкосновеността на личния живот;**
- **Поддържане на Стратегия за неприкосновеност;**
- **Поддържане на програма за неприкосновеност;**
- **Поддържане на длъжностни характеристики за лицата, отговорни за защитата на личните данни;**
- **Ангажираност на висшия мениджмънт за защита на данните на високо равнище;**
- **Разпределяне на ресурсите за адекватно прилагане на програмата за неприкосновеност (бюджет, персонал);**
- **Разпределение на отговорностите за защита на данните;**
- **Определяне на представител в държавите-членки, в които организацията не поддържа физическо присъствие – до 2018г.**
- **Провеждане на редовна комуникация между отделните длъжностни лица контролиращи и отговарящи за защитата на личните данни;**
- **Консултирайте се със заинтересованите страни в рамките на организацията по въпросите за поверителност на данните;**
- **Докладвайте, по график, за състоянието на програмата за защита на данните (например на борда на директорите, управителен съвет);**
- **Интегриране на защитата на личните данни в оценките или отчетите на риска за бизнеса;**
- **Поддържане на Кодекс за поведение;**
- **Поддържайте на ръководство по етика;**
- **Поддържане на стратегия, която да приведе дейността в съответствие с нормативните изисквания (например, противоречия в различните актове, различия в стандартите, създавайки рационално множество от правила);**
- **Изискване на служителите да приемат и се ангажират с изпълнение на политиката за защита на данните;**
- **Докладване периодично за състоянието на програмата за неприкосновеността на личния живот на външните заинтересовани страни в подходящи вид и време(например годишните доклади, трети лица, клиенти).**

ПРЕГЛЕДА НА ЛИЧНИТЕ ДАННИ

Поддържане на списък на ключовите места за съхранение на лични данни или потоците от лични

- Поддържане на списък на основните регистри на личните данни (какви личните данни, се съхраняват и къде);
- Разделянето на личните данни по типове (например лични данни, чувствителни и публични);
- Получаване на одобрение за обработка на данни (ако се изисква предварително одобрение) – проверка, (консултация след 2018)
- Регистриране на базите с лични данни в Националния орган за защита на данните (когато регистрацията е задължителна);
- Поддържане на документация за всички трансгранични потоци (трансфер) от данни (страна, правен механизъм, който се използва като основание за прехвърляне като Privacy Shield, договори и клаузи, обвързващи корпоративни правила, или одобрения от компетентните органи за защита на данните);
- Поддържане на диаграми за основните потоци от данни (например между системите, между процеси, между държави)
- Използване на задължителни фирмени правила, както и механизъм за трансфер на данни;
- Използване на стандартните договорни клаузи, като механизъм за прехвърляне на данни;
- Използване на трансгранични правила за поверителност, като механизъм за прехвърляне на данни;
- Използване на рамката на Privacy Shield като механизъм за прехвърляне на данни;
- Използване на одобрение от органа за защита на данните, като механизъм за прехвърляне на данни;

ПОЛИТИКИ ЗА НЕПРИКОСНОВЕНОСТ НА ДАННИТЕ
Поддържане на политики на защита на данните които отговаря на законовите изисквания

- Декларации за поверителност на данните;
- Поддържане на диференцирана по отношение на служителите политика за поверителност на данните – „необходимост да се знае“
- Одобрение от висшия мениджмънт за политиката на поверителност;
- Документирано правното основание за обработка на лични данни;
- Дефиниране на ръководните принципи в документа за съгласие

ПРИЛАГАНЕ НА ЗАЩИТА ПРИ ОБРАБОТКА

Поддържа оперативни политики и процедури в съответствие с политиката за поверителност

- Поддържане на политики/процедури за събирането и използването на чувствителни лични данни (включително биометрични данни);
- Поддържане на политики/процедури за поддържане на качеството на данните;
- Поддържане на политики/процедури за анонимизация на лични данни
- Поддържане на политики/процедури за преглеждане на дейностите по обработка на лични данни, извършени изцяло или частично чрез автоматизирани средства;
- Поддържане на политики/процедури за повторна (вторична, secondary) употреба на личните данни;
- Поддържане на политики/процедури за събиране на информираното (предпочитаното) съгласие;
- Поддържане на политики/процедури, предназначени за унищожаване на личните данни;
- Интегриране на защитата на личните данни в използването на бисквитки (cookies) и механизми за проследяване;
- Интегриране на защитата на личните данни в записите за практики на задържане на данните;
- Интегриране на защитата на личните данни в практиките за директен маркетинг;
- Интегриране на поверителността на данните в практиките за маркетинг по електронната поща
- Интегриране на защитата на личните данни в практиките за телемаркетинг
- Интегриране на защитата на личните данни в практиките за поведенческата реклама
- Интегриране на защитата на личните данни в практиките за наемането
- Интегриране на защитата на личните данни в практиките за проверка (проучване) на служителите
- Интегриране на защитата на личните данни в социалните медийни практики
- Интегриране на защитата на личните данни в политиките/процедурите за защита на вашите собствени мобилни (носими) устройства (Bring Your Own Device, BYOD)
- Интегриране на поверителността на личните данни в практиките за здравето и безопасността
- Интегриране на защитата на личните данни в взаимодействия с профсъюзните организации (работническите съвети) (works councils)
- Интегриране на защитата на личните данни в практики за мониторинг на служителите

ПРИЛАГАНЕ НА ЗАЩИТА ПРИ ОБРАБОТКАТА

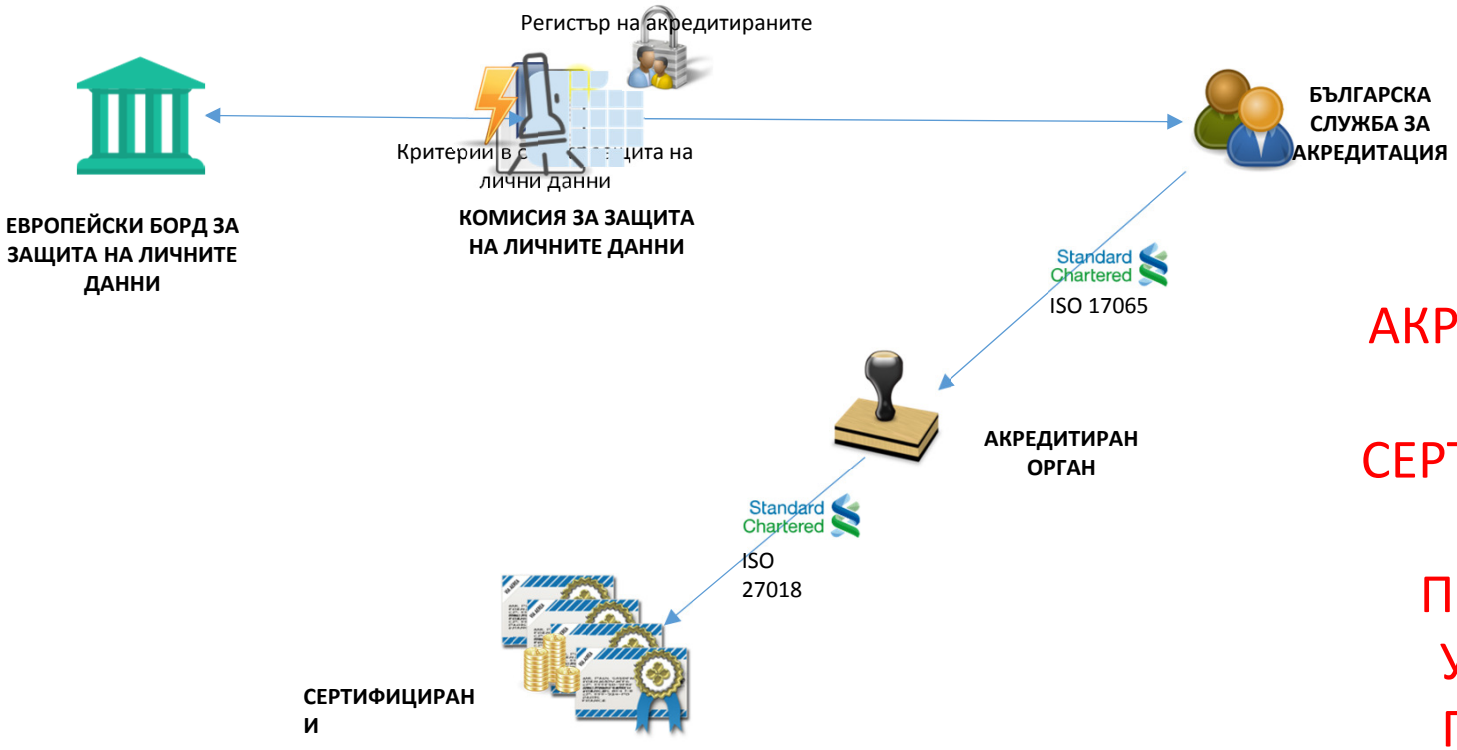
Поддържа оперативни политики и процедури в съответствие с политиката за поверителност

- Интегриране на защитата на личните данни в практиките за наблюдение на електронната поща
- Интегриране на защитата на личните данни в употреба на видеонаблюдението (CCTV)
- Интегриране на защитата на личните данни в използването на устройства определящи местоположението (проследяване и или населено място)
- Интегриране на защитата на личните данни в делегирането на достъп до акаунтите за електронна поща на служители на компанията (например при ваканция, временна нетрудоспособност/болнични, прекратяване на взаимоотношенията)
- Интегриране на защитата на личните данни в практиките за изследвания/открития в електронния свят (e-discovery)
- Интегриране на защитата на личните данни в провеждане на вътрешни разследвания/инспекции
- Интегриране на защитата на личните данни в практиките за разследване и за правоприлагане
- Интегриране на защитата на личните данни в практиките на взаимоотношенията клиент/пациент/гражданин (например продажби на дребно, предоставяне на здравно обслужване, данъчна обработка)
- Интегриране на поверителността на данните в бек офис/административните процедури (например за управление на съоръжения)
- Интегриране на защитата на личните данни в процедурите за финансови операции (например кредити, фактуриране, обработка на транзакции)
- Интегриране на защитата на личните данни в изследователските практики

СЕРТИФИЦИРАНЕ и КОДЕКСИ НА ПОВЕДЕНИЕ

- Механизми за демонстрация на съответствие с изискванията на регламента;
- Трябва да е достъпно за продукти, услуги, процеси, системи или програми;
- Механизмите следват общо установените национални правила, като КЗЛД е компетентен орган в областта на защитата на личните данни;
- Сертифицираме – механизъм на преценка на съответствие от акредитиран орган;
- Маркировка и печати – механизъм за самооценка, по критерии одобрени от компетентния орган;
- Кодекси на поведение – споделени добри практики (одобрени от компетентния орган);

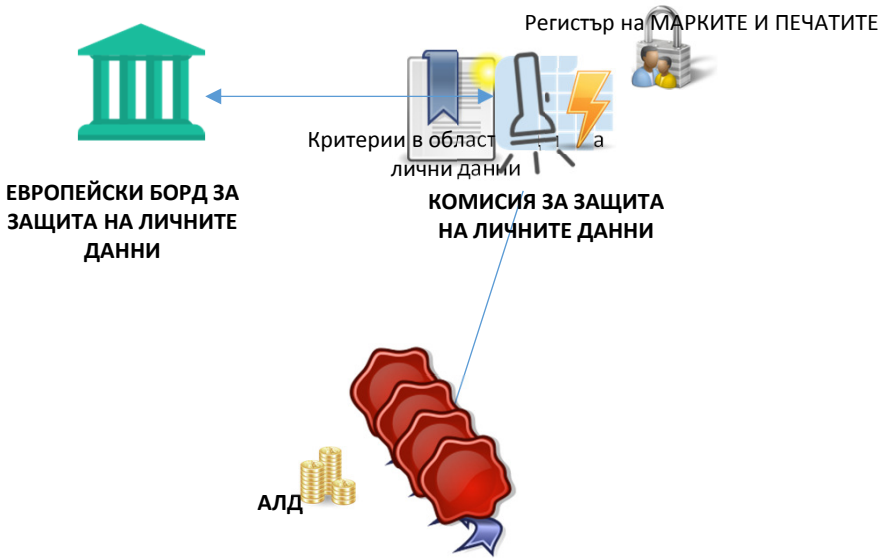
СЕРТИФИЦИРАНЕ



АКРЕДИТИРАНЕ И СЕРТИФИЦИРАНЕ НА ПРОДУКТИ, УСЛУГИ И ПРОЦЕСИ

МЕХАНИЗМИ ЗА САМООЦЕНКА

МАРКИРОВКИ И ПЕЧАТИ



КОДЕКСИ НА ПОВЕДЕНИЕ

ПОДДЪРЖАНИ РЕГИСТРИ

- От АЛД:
  - Данни за АЛД;
  - Цели на обработването;
  - Описание на категориите субекти и лични данни;
  - Категории получатели на личните данни;
  - Трансфери;
  - Срокове за съхранение;
  - Технически и организационни мерки за защита
- От Обработващия
  - Данни за обработващия и координати на АЛД;
  - Категории извършвано обработване;
  - Трансфери;
  - Технически и организационни мерки за защита.
- Регистрите са в писмена или електронна форма;
- Регистрите се предоставят при поискване;
- Изключват се предприятия с по малко от 250 служителя ако обработката не поражда висок риск или се обработват чувствителни данни

САНКЦИИ

МАКСИМАЛЕН РАЗМЕР ДО 20 000Е ИЛИ 4% ОТ ОБОРОТА

ПРЕЦЕНКА НА ДЪРЖАВАТА ЗА НАЛАГАНЕ НА ГЛОБИ НА ДЪРЖАВНИ ОРГАНИ

ЕДИННА ПОЛИТИКА ЗА ВСИЧКИ ДЪРЖАВИ ЧЛЕНКИ – КОМИТЕТЪТ ЩЕ ИЗГОТВИ НАСОКИ ЗА ПРИЛАГАНЕТО

НЕИЗПЪЛНЕНИЕ ЗАДЪЛЖЕНИЕ ОТ АДМИНИСТРАТОР	НЕ СПАЗВАНЕ ПРАВАТА НА СУБЕКТИТЕ И НАРУШЕНИЕ НА ОБЩИТЕ ПРИНЦИПИ	НЕ СПАЗВАНЕ РАЗПОРЕДБИТЕ НА НАДЗОРНИЯ ОРГАН
10 000 000Е или 2% от ОБОРОТА	**20 000 000Е или 4% от ОБОРОТА**	**20 000 000Е или 4% от ОБОРОТА**

ПРАВА НА СУБЕКТИТЕ

- Прозрачна информация, комуникация и условия за упражняването на правата на субекта на данни – чл.12
- Информация, предоставяна при събиране на лични данни от субекта на данните - чл.13;
- Информация, предоставяна, когато личните данни идват от субекта на данните – чл.14;
- Право на достъп на субекта на данните – чл.15;
- Право на коригиране – чл.16;
- Право на изтриване (право „да бъдеш забравен“) – чл.17
- Право на ограничаване на обработването – чл.18;
- Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването – чл.19;
- Право на преносимост на данните – чл.20;
- Право на възражение и автоматизирано вземане на индивидуални решения – чл.21
- Автоматизирано вземане на индивидуални решения, включително профилиране – чл.22

БЛАГОДАРЯ ЗА ВНИМАНИЕТО

ЦАНКО ЦОЛОВ

ЧЛЕН НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

tzolov@cpdp.bg