Модел за прилагане на GDPR в организациите

ЦАНКО ЦОЛОВ

Член на Комисията за защита на личните данни

tzolov@cpdp.bg

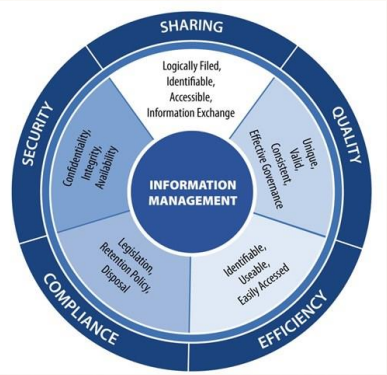
За какво ще си говорим

- Защо ни е необходима промяна
- Философия на Регламент 2016/679
- Организациите в дигиталната ера
- Какво ни трябва за да постигнем съответствие с Регламента
- Оценка на съответствието с регламент 2016/679
- Малко думи и за санкциите
- Кодекси на поведение
- Митове за GDPR

Нещо се промени около нас

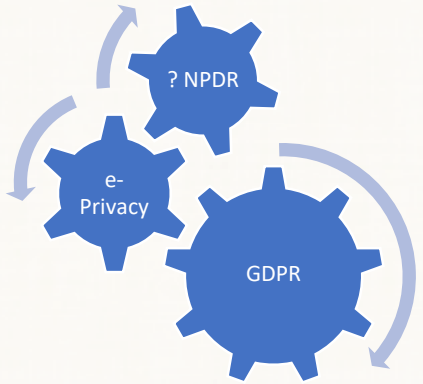
- Технологичен скок
  - Big Data – обем, скорост, разнообразие;
  - Data Analysis;
  - Internet of Things;
  - Blockchain.
- Промени се:
  - Икономиката
  - Пазарът
  - Организациите
- Трябва да се създадат правила за употреба на информацията
  - За държавата – класифицирана информация;
  - За хората – личните данни
  - За организациите – не личните данни
  - За комуникацията между тях – e-Privacy

Enterprise Information Framework



Data Driven

Digital Market



Защо ни трябва промяна

- 81% от европейците смятат, че нямат пълен контрол над личните си данни онлайн;
- 69% от европейците биха искали да дадат своето изрично одобрение преди събирането и обработката на личните им данни;
- Само 24% от европейците имат доверие на онлайн фирми като търсачки, сайтове за социални контакти и електронна поща и услуги.

Евробарометър, 2015 г.

- Застаряващо законодателство – Директива 95/46, прилагана по различен начин във всяка една страна членка;
- Противоречие на растежа – познание в интерес на бизнеса - но хората искат да управляват познанието;
- Имиджът на компанията като стратегическо предимство.

Променящ играта

Обхват

Публичен и частен
Базирани в Европа

Базирани в Целия свят

Играчи

Субекти на данни
Администратори

Обработващи
Надзорни органи

Лични данни

Пряко
Непряко

Специални

Принципи на обработка

Законосъобразност, прозрачност

Конкретни цели

Точност

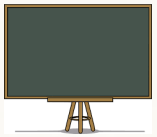
Сведени до минимум

За определен срок

Подходящо ниво на сигурност

Отчетност

Права на субектите



Право на информация

Право на достъп

Коригиране и изтриване

Ограничаване

Уведомяване

Преносимост

Възражение
Машинни решения
Профилиране

Законосъобразен процес на обработка

съгласие

договор

закон

Защита на лицето

Публичен интерес

Преобладаващ интерес

Законодателство със зъби

Санкции

Обслужване на едно гише

Завишен надзор

GDPR

Сертифициране Кодекси

Акредитация

Сертифициране

Марки и печати

Кодекси на поведение

Трансфер на данни

Стандартни договорни клаузи

Одобрени фирмени правила

Двустранни спогодби

Сертификати
Кодекси на поведение

Задължения на АЛД

Отчетност
Служител

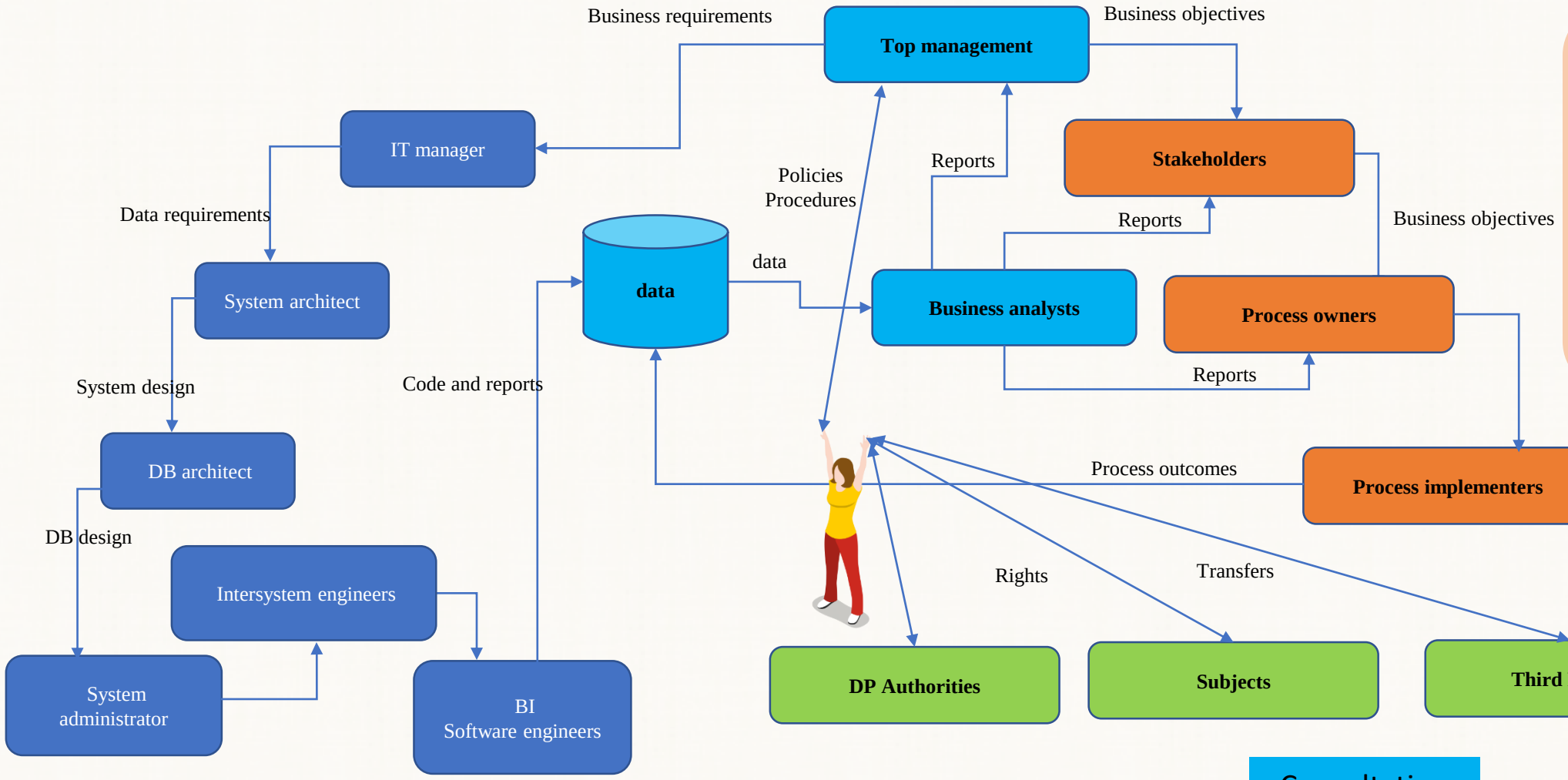
Запис на операциите

Риск анализ
Оценка на Въздействието

Неприкосновеност при проектиране
Неприкосновеност по подразбиране

Технически и организационни мерки
72 ч срок за уведомяване

Модел на организация в ерата на цифровата икономика под въздействието на GDPR



- ✓ Описание процеси;
- ✓ Поставяне цели
- ✓ Дефиниране роли;
- ✓ Дефиниране KPIs;
- ✓ Модел на данните

Business Analysis | **Data Flow** | **Gap Analysis** | **Impact Assessment** | Consultation / Code / Do nothing | **Development**

Процесът по въвеждане на GDPR малко в детайли

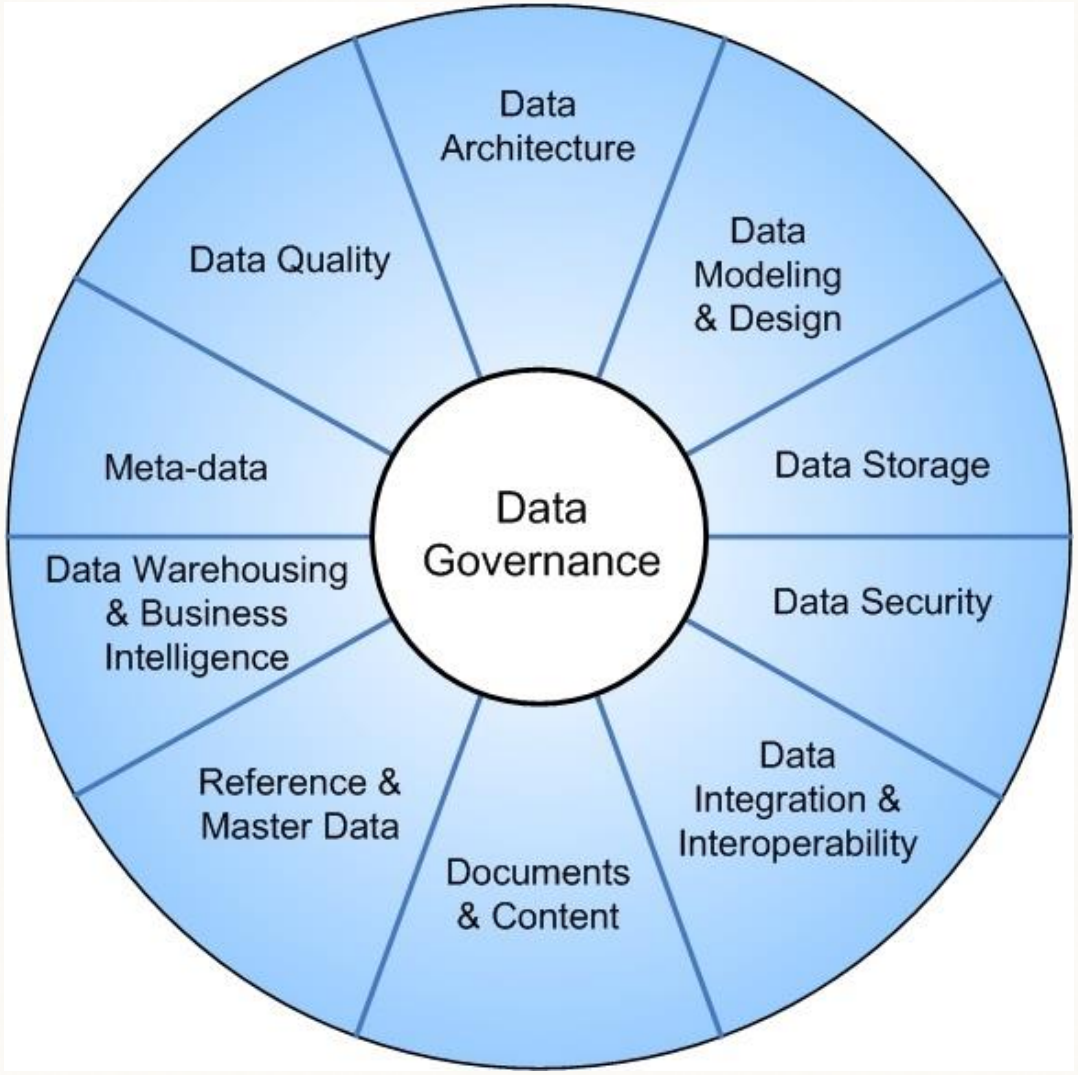
Business Analysis	Data Flow	Gap Analysis	Impact Assessment	Do nothing Consultation Code	Improvement
Какви са бизнес процесите които протичат в организацията: Наименование на процеса; Бизнес цел на процеса Съставляващи процеси – описващи алтернативи при различни изходи на логическите блокове; Собственик на процеса; **Съставляващите процеси трябва да се опишат като:** Наименование Отговорник за съставляващия процес – обработващ или АЛД Наименование на регистъра или регистрите от данни които използва; Цел на обработката Законосъобразност на обработката – Категория физически лица, чийто данни се обработват; От къде са получени данните Кой има достъп до данните – профили, базирани на роли; Схема на съставляващия процес, Трансфер на данни към външни организации.	**Регистър с данни** **Наименование;** **Тип на носителя,** **Информационна система;** **Физическо място;** **Срок за съхраняване;** **Очакван обем** **Категории данни** • физическа • физиологична • генетична • психическа • психологическа • икономическа • културна • социална • семейна • биометрични • произход и убеждения • членство • лични данни за здравето • сексуалност • IP адрес и локация	• Нови процеси • Несъответствие на съществуващите процеси с GDPR • Недостатъци на модела – роли и органи • Необходими нови технологии	• Анализ на риска – ISO 31000 – матрица на риска; • Кои са обработките пораждащи висок риск; • Мерки за намаляване на риска; • Определяне остатъчния риск; • При висок остатъчен риск – консултация; • Документация – правила и процедури	Да получим гаранции че използваните организационни и технически мерки съответстват на GDPR	

Какви способности трябва да притежаваме за да постигнем съответствие с GDPR

- Определени ли са длъжностни лица
- Наличност на план за защитата
- Извършен ли е анализ на риска и оценка на въздействието
- Наличие на политики за защита на данните
- Документиране на изискванията
- Обучение на персонала
- Осъществяване на пълен одит на обработката на данните
- изграждане на система от лог файлове
- Спазване на принципите за законосъобразност
- Минимално изискуеми данни
- Срок на съхранение
- Актуалност
- Обработвани за конкретни цели
- Поддържане на роли в организацията при обработката
- Реализация на принципа – „необходимост да се знае“
- Разпределяне на отговорности при обработката
- Къде са предоставени данните;
- Уведомяване при промяна на данните
- Уведомяване при блокиране и изтриване

- Какви са потоците от данни
- Какви са правилата по които те се обработват
- Неприкосновеност по подразбиране
- Неприкосновеност при проектиране
- Управление на всички налични бази от данни
- Отстраняване на излишната информация
- Различаване режима на обработка в зависимост от класификацията
- Физическо разполагане на данните
- Разпознаваме на лични данни
- Класифицираме документи и записи с лични данни
- Определяме типа на личните данни
- Разпознаване на нови колекции от данни;
- Профилиране и машинно вземане на решение;
- Анонимизация на данните.
- Поддържане на речник за мета данни
- Валидност на обработката
- Задължения на администратора
- Трансфер на данни

Какви способности трябва да притежаваме за да постигнем съответствие с GDPR



Document and Content management

Data Warehouse management

Meta Data management

Data Architecture management

Data Quality management

Business Intelligence management

Reference and Master Data management

Data Development

Database Operations management

Data Security management

ОЦЕНКА НА СЪОТВЕТСТВИЕ С РЕГЛАМЕНТА

1. Управленска структура;
2. Преглед и класификация на личните данни;
3. Политики за неприкосновеност на данните;
4. Прилагане на защитата при обработката;
5. Програма за обучение;
6. Управление на риска за информационната сигурност;
7. **Управление на риска от трети страни**;
8. Уведомления при пробив в системата;
9. Поддържане процедури за запитвания и жалби;
10. Мониторинг за нови оперативни практики;
11. Програма за управление на нарушенията;
12. Мониторинг на процедурите за обработване;
13. Следене на външни критерии

УПРАВЛЕНИЕ НА РИСКА ОТ ТРЕТИ СТРАНИ

Поддържане на договори и споразумения с трети страни и техните партньори, в съответствие с политиката за поверителност на данните, правните изисквания, както допустимия толериран на риска

- Поддържане на изискванията за поверителност на данните за трети страни (напр., доставчици, изпълнители, разработчици, филиали);
- Поддържане на процедури за изпълнение на договори или споразумения с всички изпълнители;
- Поддържане на процедура за оценка на риска за осигуряване на поверителността на данните от всеки доставчик;
- Провеждане на надлежна проверка за осигуряването на сигурността на данните и състоянието на сигурността от потенциалните доставчици/изпълнители;
- Поддържане на една политика, уреждаща отношенията с облачни доставчици (cloud providers);
- Поддържане процедури за справяне (решаване) на случаи на неспазване на договори и споразумения;
- Провеждане на надлежна проверка за осигуряването на сигурността на данните и състоянието на сигурността от потенциалните доставчици/изпълнители на основата на оценка на риска;
- Преглед на дългосрочни договори за нови или развиващи рискове за защита на данните;

АДМИНИСТРАТИВНИ САНКЦИИ

МАКСИМАЛЕН РАЗМЕР ДО 20 000 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**

Какво е КОДЕКС

- Кодексите на поведение са **добри или лоши практики** които се задължаваме да прилагаме или никога да не използваме;
- Кодексите за поведение имат за **цел** да допринесат за правилното прилагане на настоящия регламент, като се отчитат специфичните характеристики на различните обработващи данни **сектори** и конкретните нужди на **микропредприятията, малките и средните предприятия**.

ФИЛОСОФИЯ на КОДЕКСИ НА ПОВЕДЕНИЕ

Какво включва КОДЕКСА НА ПОВЕДЕНИЕ

- добросъвестното и прозрачно обработване;
- законните интереси, преследвани от администраторите в конкретни аспекти;
- събирането на лични данни;
- псевдонимизацията на лични данни;
- информирането на обществеността и на субектите на данни;
- упражняването на правата на субектите на данни;
- информирането и закрилата на децата и начина за получаване на съгласие от носещите родителска отговорност за детето;
- мерките и процедурите за неприкосновеност по подразбиране и проектиране както и сигурност на обработването;
- уведомяването на надзорните органи за нарушения на сигурността на личните данни и съобщаването за такива нарушения на сигурността на личните данни на субектите на данни;
- предаването на лични данни на трети държави или международни организации; или
- извънсъдебните производства и другите процедури за разрешаване на спорове между администраторите и субектите на данни по отношение на обработването.

Какво още ни трябва за да функционира КОДЕКСЪТ

- КОДЕКСЪТ се наблюдава от акредитиран орган;
- Към кодекса могат да се присъединяват трети страни (при използване механизма на двустранен договор) и извън територията на трети страни;
- Кодексът е одобрен от националния надзорен орган;
- Кодексът е одобрен от Комитета когато засяга повече от една държава членка;
- Одобряващият орган осигурява публичност на КОДЕКСА

Какви са големите ползи от КОДЕКСА

- Може да се използва като основание за трансфер на данни;
- Може да се използва като доказателство за използването на подходящи мерки за доказване на съответствието;
- Може да гарантира спазването на изискването на регламент 2016/679 от обработващите;
- Може да установява параметри на задълженията на администратора и обработващия;
- Може да докаже отчитането на мнението на субектите на данни;
- Може да послужи като буфер между субекта на данни и надзора;
- Може да се използва като доказателство за намаляване на потенциални глоби и санкции
- Може да ограничи правата на субектите при разследване нарушение на кодекса

МИТОВЕ ЗА GDPR

- Регулацията не се отнася за нас;
- GDPR е защита от външни атаки - преди всичко права и задължения – **„неприкосновеност # сигурност“**;
- GDPR не е само борба с хакерите – GDPR е **свободно движение на данни при зачитане на правото на защита**.
- Съгласието винаги е **изрично** – не то е **недвусмислено;**
- Въвеждането на Регулацията е отговорност на IT отдела – преди всичко на бизнеса;
- GDPR са санкции – не това е **начин на правене на бизнес**;
- Регулацията няма да започне да действа на 25 май 2018г.;
- Не се отнася до мен защото съм само обработващ на лични данни;
- Съответствието с GDPR веднаж постигнато е „достатъчно“ – съответствието е процес;
- Правата на лицата са абсолютни – не и ако съществува друго **законово задължение** за обработка;
- Профилирането изисква съгласие – не ако не произвежда „**правни последствия**“ или „**значително ви засяга**“;
- Псевдоанонимизираните данни се обработват като всички останали данни – не ако те са **надеждно** псевдоанонимизирани.


GDPR Fines: 4% of global turnover
Privacy Budget: 0.0004% of global turnover
Да помислим

Цанко Цолов
член на Комисията за защита на личните данни
tzolov@cpdp.bg