



Съфинансирано от
Европейския съюз



ПРОГРАМА
НАУЧНИ ИЗСЛЕДВАНИЯ,
ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА
ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ

НАЦИОНАЛНА РАМКА ЗА УПРАВЛЕНИЕ НА ДАННИТЕ

Проект BG16RFPR002-2.010-0001, „Изграждане на стратегическа, организационна и техническа рамка за управление на данни и оперативна съвместимост“ (D1) по административен договор № BG16RP002-2.010-0001-C02 директно предоставяне на безвъзмездна финансова помощ, финансиран от програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021/2027 г., съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.



История на промените

Дата	Издание	Описание	Автор
21.04.2022	A	Начално издание	Екип на Световната банка
12.06.2025	A	Актуализирана версия, съобразно препоръки на Възложителя	Екип на Световната банка
06.11.2025	A	Локализация	Екип за управление на проекта

Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от Министерство на електронното управление и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган.



СЪДЪРЖАНИЕ

СЪКРАЩЕНИЯ	5
I. РЕЗЮМЕ.....	8
1. Цели на НРУД	8
2. Текущо състояние и предизвикателства	8
3. Структура на НРУД	9
II. ВЪВЕДЕНИЕ	10
1. Контекст на управлението на данни в България	11
2. Цели на НРУД	13
3. Структура на НРУД	14
III. НАЦИОНАЛНА РЕФЕРЕНТНА РАМКА ЗА УПРАВЛЕНИЕ НА ДАННИ	16
1. КАТЕГОРИЯ ИНСТИТУЦИИ.....	19
1.1 Описание	19
1.2 Цел	19
1.3 Рискове	20
1.4 Изисквания за съответствие	20
1.5 Елементи на категорията ИНСТИТУЦИИ	21
1.5.1. Стратегия.....	21
1.5.2. Ангажимент на високо ниво	23
1.5.3. Организация.....	24
1.5.4. Отчетност	26
1.5.5. Подкрепа и застъпничество за използване на данните.....	27
1.5.6. Стратегия за уменията	28
2. КАТЕГОРИЯ ПОЛИТИКИ	29
2.1 Описание	29
2.2 Цел	30
2.3 Рискове	30
2.4 Изисквания за съответствие	31
2.5 Елементи на категорията ПОЛИТИКИ.....	32
2.5.1 Политика за съхранение на данните.....	32
2.5.2 Стандарти за метаданни	34
2.5.3 Защита на данните.....	36
2.5.4 Интегритет на данните.....	37
2.5.5 Стандарти за данни	39
2.5.6 Прозрачност на алгоритмите	40
2.5.7 Регулаторно съответствие	41
2.5.8 Суверенитет на данните.....	43
2.5.9 Базови регистри	45
3. КАТЕГОРИЯ ПРОЦЕСИ.....	46
3.1 Описание	46



3.2 Цел	46
3.3 Рискове	47
3.4 Изисквания за съответствие	48
3.5 Елементи на категорията ПРОЦЕСИ	49
3.5.1 Поддръжка на данните.....	49
3.5.2 Управление на качеството на данните	50
3.5.3 Управление на инциденти	52
3.5.4 Управление на промените	53
3.5.5 Откриване на данни	55
3.5.6 Процес на формулиране	56
3.5.7 Прилагане на политиките	57
3.5.8 Мониторинг	58
3.5.9 Управление на жизнения цикъл на данните	59
3.5.10 Координация	60
3.5.11 Управление на доверието	62
4. КАТЕГОРИЯ ТЕХНОЛОГИИ	63
4.1.Описание	63
4.2.Цел	63
4.3.Рискове	64
4.4.Изисквания за съответствие	65
4.5.Елементи на категорията ТЕХНОЛОГИИ.....	66
4.5.1 Инструменти за управление на метаданни (Каталог от данни)..	66
4.5.2 Инструменти за управление на процесите, свързани с данни	67
4.5.3 Проследяване на данните	68
4.5.4 Достъп и сигурност	70
4.5.5 Инструменти за управление на качеството на данните.....	71
4.5.6 Основни/референтни данни	72
4.5.7 Системна архитектура	73

Приложения (отделен документ):

Приложение 1. Референтна матрица RACI

Приложение 2. Примерни КПИ за измерване на напредъка

Приложение 3. Методология за качество на данните

Приложение 4. Референтен списък със стандарти за данните

Приложение 5. Референтен списък на онтологиите

Приложение 6. Референтна системна архитектура за управление на данни



СЪКРАЩЕНИЯ

AIDA	Акт за изкуствения интелект и данните
B2G	Бизнес към държавната администрация
CDMP	Сертифициран специалист по управление на данни
CGMES	Стандарт за модела на обмен в обществената мрежа
CIM	Общ информационен модел
CIPP/E	Сертифициран специалист по конфиденциалност на информацията
DCAT-AP	Приложение за портали за данни в Европа
DESI	Индекс за навлизането на цифровите технологии в икономиката и обществото
DID	Децентрализиран идентификатор
DNS	Система за имена на домейните
DOI	Идентификатор на цифров обект
DPO	Длъжностно лице по защита на данните
ЕК	Европейска комисия
ENTSO-E	Европейска асоциация на операторите на преносни системи за електроенергия
ЕС	Европейски съюз
FGDC	Федерален комитет за географски данни
GDDS	Система за разпространение на данни
ОРЗД	Общ регламент относно защитата на данните
IETF	Работна група по интернет инженерство
IoT	Интернет на нещата
IRI	Еднозначен идентификатор на ресурс
ISZR	Информационна система за основни регистри (<i>Informační systém základních registrů</i>)
KKSzB	Унгарска централна правителствена сервизна шина (<i>Központi Kormányzati Szolgáltatás Busz – KKSzB</i>)
LDQD	Измерения на качеството на свързаните данни



MARC	Машинно-четимо каталогизиране
MDM	Управление на основни данни
MDM/RDM	Управление на основни и референтни данни
MFA	Многофакторно удостоверяване
NSDP	Национална страница с обобщени данни
OLS	Услуга за търсене на онтологии
OPSI	Обсерватория за иновации в публичния сектор
OSI	Взаимосвързаност на отворени системи
PCTF	Пан-канадската рамка за доверие
PIPEDA	Закон за електронните документи и защита на личната информация
RACI	Responsible, Accountable, Consulted, Informed (отговорен, отчетен, консултиран, информиран)
RBAC	Критерии за достъп базирани на ролята
RDF	Рамка за описание на ресурсите
SDMX	Стандарт за обмен на статистически данни и метаданни
SIMS	Единна интегрирана структура за метаданни
SSO	Еднократно влизане
URI	Универсален идентификатор на ресурси
URL	Унифициран указател на ресурс
URN	Унифицирано наименование на ресурс
W3C	Консорциум за световната Интернет мрежа
AOB	Алгоритмична оценка на въздействието
АУД	Акт за управление на данните
АЦП	Акт за цифровите пазари
АЦУ	Акт за цифровите услуги
БНБ	Българска народна банка
ВКУ	Възмездни консултантски услуги
ЕКИД	Европейски комитет за иновации в областта на данните
ЕПЗД	Европейско пространство за здравни данни
ЕРОС	Европейска рамка за оперативна съвместимост



ИИ	Изкуствен интелект
ИКЕ на ООН	Икономическа комисия за Европа на Организацията на обединените нации
ИПА	Институт по публична администрация
КПИ	Ключов показател за изпълнение
МВФ	Международен валутен фонд
МЕК	Международна електротехническа комисия
МЕУ	Министерство на електронното управление
МС	Министерски съвет
МСП	Малки и средни предприятия
НДУД	Национална дирекция за управление на данните
НКО	Национален компетентен орган
НПО	Неправителствена организация
НРД	Национален речник на данните
НРУД	Национална рамка за управление на данните
НСИ	Национален статистически институт
ПНИИДИТ	Програма за научни изследвания, иновации и дигитализация за интелигентна трансформация
ППИ	Приложно-програмен интерфейс
РУД	Рамка за управление на данните
РчКД	Речник за качеството на данните
ССРДПлюс	Специален стандарт за разпространение на данни Плюс
СЦТ	Служба по цифрова трансформация
УЖЦД	Управление на жизнения цикъл на данните
ЦВВ	Цел за време за възстановяване
ЦПС	Цифров публичен сектор



I. РЕЗЮМЕ

1. Цели на НРУД

Националната референтна рамка за управление на данни (НРУД) има за цел да подобри управлението на данните и да засили тяхното използване в публичния сектор на Република България. Рамката също така цели да повиши качеството, оперативната съвместимост и сигурността на данните, като едновременно с това насърчава култура на вземане на решения, основани на данни, и предоставяне на услуги, ориентирани към гражданите, в съответствие с международните добри практики и европейските регулации. Освен това тя има за цел да стимулира използването и повторното използване на данни от публичния и частния сектор за насърчаване на икономическия растеж и създаване на работни места.

НРУД предоставя общ преглед на глобалната и европейска рамка за управлението на данните и предлага препоръки, които да подпомогнат прилагането на рамката за управление на данните, основана на обширни изследвания, анализ на международни примери и консултации с екосистема от заинтересовани страни в България.

2. Текущо състояние и предизвикателства

С напредъка на България към постигане на цифрова зрялост и съответствие с Европейската стратегия за данните, Акта за управление на данните (АУД) и Директивата за отворените данни, страната е изправена както пред нови възможности, така и пред структурни предизвикателства при използването на данните за постигане на по-добри обществени резултати.

Фрагментираните отговорности, свързани с управлението на данните, различният административен капацитет на институциите и пропуските в правното съответствие възпрепятстват ефективното повторно използване на данните, както и осигуряването на тяхното качество и прозрачност.

НРУД разглежда тези предизвикателства чрез подход, основан на три основни принципа: устойчивост, мащабируемост и гъвкавост, и оперативна съвместимост.

Целта на рамката е да установи цялостен модел за управление на данните, който да предоставя на институциите възможност да ги управляват по по-



ефективен, сигурен и прозрачен начин — с отчетност и в съответствие с изискванията на закона. По този начин се създава обществена стойност и се улеснява участието на България в екосистемата на европейските пространства от данни.

3. Структура на НРУД

НРУД е структурирана в четири основни категории: **институции, политики, процеси и технологии**. Всяка категория обхваща специфични елементи, които са от съществено значение за ефективното управление на данните. Рамката служи като цялостна концепция за изграждане на институционални механизми, нормативна основа, системи за повишаване на капацитета, технологични инструменти и процесни реформи, които да гарантират устойчиво, оперативно съвместимо и ориентирано към гражданите управление на данни.

Таблица 1. Структура на НРУД

Институции	Категорията се фокусира върху изграждането на стабилна институционална структура с централен координиращ орган, ясно определени роли и отговорности — главен служител по данните (Chief Data Officer), главен отговорник за данни (Chief Data Steward), собственици на данни (Data Owners) и отговорници за данни (Data Stewards) — както и ефективни механизми за отчетност и участие на заинтересованите страни. Препоръчва се поетапен подход, започващ с области с високо въздействие и постепенно разширяване към други сектори.
Политики	Категорията очертава основните политики, свързани със съхранението на данните, стандарти за метаданни, защита на данните, стандарти за данни, прозрачност на алгоритмите, регулаторно съответствие и суверенитет на данните. Тези политики имат за цел да гарантират качеството, сигурността и съответствието на данните с националните и с международните регулаторни изисквания. Рамката подчертава важността на



	съгласуването на националните политики с разпоредбите на ЕС и с най-добрите международни практики.
Процеси	Категорията дефинира стандартизирани процеси за поддръжка на данни, управление на качеството на данните, управление на инциденти, контрол на промените, откриване на данни, дефиниране на данни, контрол по прилагане на политиките, мониторинг и управление на жизнения цикъл на данните. Тези процеси имат за цел да оптимизират операциите с данни, да сведат до минимум рисковете и да гарантират последователност в работата с данни във всички институции от публичния сектор.
Технологии	Категорията е фокусирана върху използването на технологии в подкрепа на дейностите по управление на данните. Препоръчва се прилагането на инструменти за управление на метаданни (каталози от данни), инструменти за управление на данни, инструменти за проследяване на произхода на данните, надеждни механизми за достъп и сигурност, инструменти за управление на качеството на данните, системи за управление на основни/референтни данни и добре дефинирана системна архитектура, която насърчава оперативната съвместимост. Рамката набляга на използването на отворени стандарти и софтуерни решения с отворен код, с цел подобряване на оперативната съвместимост и намаляване на зависимостта от конкретни доставчици.

II. ВЪВЕДЕНИЕ

Настоящият документ представя национална референтна рамка за управление на данни в публичния сектор на България, която има за цел да предостави практически насоки за подобряване на качеството и управлението на данните във всички сектори и нива на управление. Приложенията към рамката съдържат преглед на глобалните и европейските политики в областта на управлението на данни и отчитат значителния напредък на България в



цифровизацията, като подчертават ключовата роля на ефективното управление на данните за постигане на националните икономически и социални цели. В същото време документът акцентира върху необходимостта от по-съгласуван, стандартизиран и оперативно съвместим подход към управлението на данните, за да се разгърне напълно техният потенциал като стратегически актив на публичния сектор.

1. Контекст на управлението на данни в България

България, преминава през бърза цифрова трансформация, водена от технологичния напредък и нарастващото значение на данните във всички аспекти на обществения живот. Публичният сектор играе ключова роля в този процес, като управлява огромни и критично важни масиви от данни, свързани с граждани, бизнес и обществени услуги. По тази причина, ефективното управление на данните не е просто технически въпрос, а основна предпоставка за ефективни, прозрачни, отговорни и ориентирани към гражданите публични услуги и процеси.

Настоящото състояние на управлението на данни в България се характеризира с комбинация от силни страни и предизвикателства. България е постигнала значителен напредък в изграждането на правна рамка за защита и отваряне на данните, в съответствие с директивите и регламентите на Европейския съюз. Създаването на портали за пространствени и отворени данни, както и инициативите за споделяне на данни, представляват важни стъпки към по-прозрачен и ориентиран към данните публичен сектор.

Страната разполага и с цифрови базови регистри, съдържащи ключова информация за граждани, бизнеси и организации. Въпреки това, тези регистри често не осигуряват необходимото качество и оперативна съвместимост, което затруднява ефективния обмен и повторното използване на данни между институциите.

Съществуват и редица предизвикателства, които възпрепятстват реализирането на пълния потенциал на последователното и устойчиво управление на данните, включително:

- **Фрагментирани данни/изолирани системи от данни:** често данните са разпределени между отделни държавни агенции и системи, което води до



неефективност, дублиране на усилия и трудности за достъп до цялостен поглед върху информацията. Липсата на оперативна съвместимост между системите възпрепятства обмена и повторната употреба на данни и затруднява предоставянето на интегрирани услуги.

- **Проблеми, свързани с качеството на данните:** непоследователните дефиниции, непълните записи и неточностите в наборите от данни компрометират надеждността на информацията, използвана в управлението на публичния сектор. Ниското качество на данните може да доведе до неправилни политически решения, неефективно предоставяне на услуги и намалено обществено доверие.
- **Ограничена оперативна съвместимост:** липсата на стандартизирани формати на данните, схеми за метаданни и приложно-програмни интерфейси възпрепятства безпроблемния обмен на данни между различните системи и институции. Това ограничава възможността за интегриране на данни от различни източници и възпрепятства развитието на цялостни и интегрирани публични услуги.
- **Пропуски по отношение на капацитета:** недостигът на квалифициран персонал с опит в управлението и анализа на данни представлява сериозно предизвикателство. Липсата на обучение и на инициативи за изграждане на капацитет ограничава възможностите на организациите от публичния сектор да управляват и да използват своите информационни активи по ефективен начин.
- **Недостатъчно регулаторно съответствие:** въпреки постигнатия напредък в хармонизация на правната рамка в България с директивите на ЕС, са необходими допълнителни усилия, за да се гарантира, че всички аспекти на управлението на данните са взети под внимание и добрите практики се прилагат по адекватен начин. Това включва изясняване на ролите и отговорностите, установяване на ясни механизми за отчетност и определяне на стандарти за качество, сигурност и оперативна съвместимост на данните.



2. Цели на НРУД

Основните цели на тази рамка са да подобри качеството на данните чрез подобряване на точността, пълнотата, съгласуваността и актуалността на данните във всички държавни институции. Това включва установяване на ясни стандарти за качество на данните, прилагане на процеси за валидиране и почистване на данни, както и насърчаване на култура на управление на качеството на данните. Друга важна цел е повишаването на оперативната съвместимост за осигуряване на безпрепятствен обмен и повторна употреба на данни между институции и системи. Това включва възприемане на стандартизирани формати на данните, схеми за метаданни и приложно-програмни интерфейси (API), както и насърчаване на използването на стандарти за отворени данни.

Освен това рамката има за цел едновременно да овласти публичния сектор и да повиши отчетността, като определя ясни роли и отговорности в управлението на данните и гарантира, че всички участници носят отговорност за своите действия. Това включва ясно разпределение на собствеността и управлението на данните, механизми за отчетност и процеси за мониторинг на съответствието. Тя също така цели повишаване на сигурността на данните чрез защита на публичните информационни активи от неоторизиран достъп, използване, разкриване, промяна или унищожаване. Това се постига чрез надеждни мерки за сигурност, ясни политики за контрол на достъпа и обучения относно най-добрите практики за защита на данните.

Друга ключова цел е повишаването на прозрачността в управлението на данните, което ще допринесе за по-голямо обществено доверие в тяхното използване. Това включва публикуване на политики за управление на данни, разширяване на достъпа до информационни активи и осигуряване на яснота относно начина на използване на данните.

Рамката е и икономически обоснована, тъй като има потенциал да стимулира растежа и иновациите чрез по-ефективно и ефикасно използване на данните.

Наред с това се предвижда изграждане на капацитет чрез развитие на уменията и експертизата, необходими за ефективно управление и използване на



данните в публичния сектор. Това включва обучителни програми, схеми за сертифициране и насърчаване на култура на грамотност при работа с данни.

3. Структура на НРУД

Настоящият документ предоставя цялостна и практична НРУД.

Въведението предоставя контекст, очертава предизвикателствата и възможностите, свързани с управлението на данни в България, и формулира целите на рамката.

Основната част предоставя подробно описание на предложената НРУД, очертавайки нейните основни принципи, ключови компоненти (институции, политики, процеси, технологии) и насоки за прилагане - представяйки структуриран подход към управлението на данните като публичен актив.

Приложенията предоставят допълнителна информация, включително подробни примери за ключови показатели за изпълнение (КПИ), матрици RACI (Responsible – Изпълнител, Accountable – Отговорен за резултата, Consulted – Консултиран, Informed – Уведомен), методология за качество на данните и списъци със съответните стандарти и онтологии.

НРУД и приложенията към нея са предназначени да служат като ресурс за разработващите политики, за държавните служители и за други заинтересовани страни, които участват във формирането на екосистемата за управление на данни в България. Целта на документите е да очертаят ясен и практически приложим подход за изграждане на по-ефективен и прозрачен публичен сектор, който базира дейността си на данни и отговаря по-ефективно на нуждите на гражданите.

Успешното прилагане на НРУД изисква активното участие и сътрудничество между широк спектър от заинтересовани страни, в т.ч. държавни институции, разработващи политики, специалисти по данни, заинтересовани страни от частния сектор и граждански организации.

Всяка група заинтересовани страни има ключова роля за осигуряване на ефективното управление на данните:

- **Разработчици на политики:** разработчиците на политики играят ключова роля в управлението на цифровата трансформация на публичния сектор. Тяхната отговорност включва осигуряване на



ефективно лидерство, координация между институциите, гарантиране на необходимите финансови и човешки ресурси, приемане на законодателство, което подкрепя целите на НРУД, както и създаване на механизми за надзор и отчетност, гарантиращи спазването на установените изисквания.

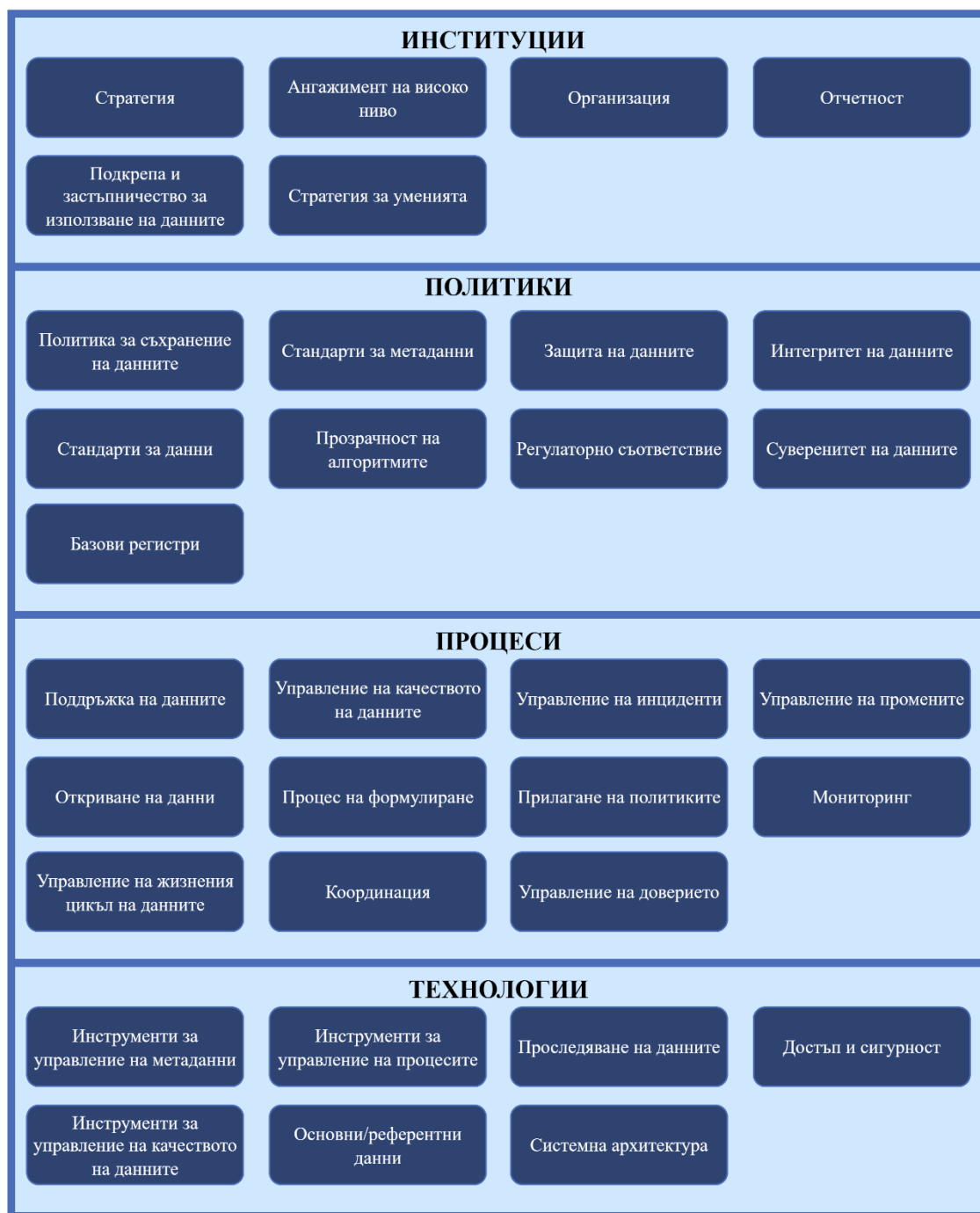
- **Държавни институции:** държавните институции отговарят за прилагането на НРУД в рамките на своята компетентност. Това включва създаване на структури за управление на данните, разработване и прилагане на политики за данните и гарантиране на съответствие със стандартите за качество, сигурност и оперативна съвместимост на данните. Институциите следва също да инвестират в изграждане на капацитет и обучения, за да осигурят на служителите си необходимите знания и умения за ефективно управление на данните.
- **Специалисти по данните:** специалистите по данни, включително отговорниците за данни (data stewards), мениджърите на данни и анализаторите на данни, отговарят за ежедневното управление на активите от данни. Те играят ключова роля за осигуряване на качеството, сигурността и оперативната съвместимост на данните, както и за насърчаване на култура на вземане на решения, основани на данни в рамките на своите организации.
- **Заинтересовани страни от частния сектор:** заинтересованите страни от частния сектор, включително представители на бизнеса и индустрията, са от съществено значение за стимулиране на иновациите и икономическия растеж чрез използването и повторното използване на данни. Те могат да допринесат чрез споделяне на най-добри практики, инвестиции в технологии, основани на данни и чрез сътрудничество с организации от публичния сектор за разработване и прилагане на ефективни рамки за управление на данните. Тяхното участие гарантира, че политиките за управление на данните са съобразени с нуждите на пазара и насърчават устойчивото развитие.



- **Граждански организации:** гражданските организации могат да предоставят ценна обратна връзка и препоръки относно политиките и практиките за управление на данните. Те също така играят важна роля в отстояването на прозрачност, отчетност и защита на правата на гражданите при използването на данни.

III. НАЦИОНАЛНА РЕФЕРЕНТНА РАМКА ЗА УПРАВЛЕНИЕ НА ДАННИ

Настоящата глава представя Националната референтна рамка за управление на данни, като формулира нейните основни принципи, ключови компоненти и насоки за прилагане. Рамката предоставя систематизиран и координиран подход към управлението на данните като стратегически публичен актив, осигурявайки тяхната цялост, сигурност, достъпност и качество в съответствие с националните и международните стандарти. Рамката определя институционалните роли и отговорности, както и необходимите политики, процеси и технологични решения, които подпомагат ефективното, прозрачно и устойчиво управление на данните в публичния сектор. Изградена върху принципите на устойчивост, мащабируемост и оперативна съвместимост, тя служи като инструмент за насърчаване на интегриран и последователен подход към управлението на данни във всички административни нива. Чрез укрепване на доверието, осигуряване на регулаторно съответствие и стимулиране на иновативни практики, рамката подпомага вземането на решения, основани на данни, подобрява качеството и ефективността на публичните услуги и допринася за икономическото и социалното развитие на Република България.



Фигура 1. Национална референтна рамка за управление на данни

Основните принципи на НРУД – устойчивост, мащабируемост, гъвкавост и оперативна съвместимост – гарантират, че стратегиите за управление на данните са стабилни, адаптивни и ефективни в дългосрочен план.



Принципът на устойчивост подчертава необходимостта практиките и инфраструктурата за управление на данни да бъдат ресурсно ефективни и екологично съобразени, осигурявайки тяхната трайност и приложимост във времето. Той насърчава използването на щадящи околната среда и икономически ефективни решения, които ограничават разхищението на ресурси и повишават оперативната ефективност.

Чрез интегриране на устойчиви практики организациите подготвят своите системи за бъдещето, като едновременно намаляват екологичния си отпечатък и повишават устойчивостта на управлението на данните.

Масшабируемостта, гъвкавостта и оперативната съвместимост са от решаващо значение за справяне с нарастващата сложност на екосистемите от данни. Масшабируемостта гарантира, че с нарастването на обемите от данни и усложняването на екосистемата от данни, НРУД може да отговори на повишените изисквания, да поддържа разнообразни или нововъзникващи обществени услуги и да се адаптира към променящи се технологични изисквания. Гъвкавостта позволява приспособяване към регулаторни промени, бизнес трансформации и технологичен напредък, като така рамката запазва своята актуалност във времето. В същото време оперативната съвместимост улеснява безпроблемния обмен и интеграцията на данни между различни платформи, системи и приложения. Тя гарантира, че структурите за управление на данните насърчават взаимната свързаност, позволявайки на организациите да споделят и използват данни по ефективен начин в множество среди, подкрепяйки информираното вземане на решения и стратегическите иновации.

НРУД е структурирана в четири ключови категории: институции, политики, процеси и технологии, като всяка от тях включва множество елементи, необходими за ефективното управление на данните. Всяка категория включва описание, цел, свързани рискове и кратък списък с изисквания за съответствие, с цел да се гарантира яснота при прилагането. В рамките на тези категории, елементите са систематично представени с кратко описание, което очертава конкретната им роля в НРУД. Освен това за всеки елемент са ясно определени обхватът и сферите на приложение, с цел по-добро разбиране на тяхното



въздействие и приложимост. Този структуриран подход предлага ясна, систематична и мащабируема методология, която позволява на организациите ефективно да въвеждат и поддържат практики за управление на данни, като едновременно с това отчитат свързаните рискове и гарантират спазването на изискванията за съответствие.

1. КАТЕГОРИЯ ИНСТИТУЦИИ

1.1 Описание

Категорията ИНСТИТУЦИИ на НРУД обхваща изграждането на стабилна и отговорна структура на управление чрез определяне на стратегия и ангажимент на различни нива. Тя подчертава значението на стратегическото съгласуване, силното лидерство и ясната организационна структура за осигуряването на устойчива система за управление на данните. Тази категория разглежда необходимостта от квалифициран персонал, последователно застъпничество за управление на данните и насърчаване на култура на съответствие и отчетност. Включени са стратегии за ангажиране на заинтересованите страни, застъпничество и обучение за създаване на устойчив модел на управление, който утвърждава стойността на данните като публичен актив.

1.2 Цел

Основната цел на категорията ИНСТИТУЦИИ е да създаде основа от стратегически усилия, отчетност и ангажираност, необходими за ефективното прилагане и устойчивостта на инициативите за управление на данни. Тя гарантира, че всички заинтересовани страни в съответствие с НРУД, разбират ролите си и разполагат с необходимите ресурси за изпълнение на отговорностите си. Чрез насърчаване на култура на отговорност за данните (data stewardship) и застъпничество, тази категория има за цел да изгради ангажираност на всички организационни нива, от ангажимент на високо ниво до отделните специалисти по данни, като гарантира, че практиките за управление на данните се прилагат в ежедневните дейности и при вземането на решения на стратегическо ниво.



1.3 Рискове

Прилагането на НРУД носи редица предизвикателства, които организациите следва да предприемат превантивни мерки, за да гарантират ефективност и устойчивост. Един от основните рискове е съпротивата срещу промените, при която служителите и организациите проявяват нежелание да възприемат нови подходи и стандарти за управление на данните, което може да забави изпълнението и да намали нивото на съответствие. Освен това, ограниченията, свързани с ресурсите, като например ограничено финансиране, персонал или технически опит, могат да възпрепятстват развитието и дългосрочната устойчивост на инициативите за управление. Честата смяна на ръководството представлява още един риск, тъй като промените в ръководството могат да нарушат приемствеността в управлението, да намалят стратегическата подкрепа и да доведат до промяна на приоритетите, подкопавайки дългосрочните ангажименти.

Освен това, неяснотата по отношение на ролите и отговорностите в рамките на управленските структури може да доведе до неефективност, неправилно управление и пропуски в отчетността, което отслабва цялостната рамка. Неспазването на политиките за управление на данните увеличава риска от пробиви в сигурността, правни последици и увреждане на репутацията. Неспазването на установените протоколи може да компрометира целостта и сигурността на данните, излагайки организациите на регулаторни санкции и загуба на обществено доверие. Преодоляването на тези рискове и успешното прилагане на рамката изисква ясна комуникация, целенасочено осигуряване на ресурси и лидерски ангажимент.

1.4 Изисквания за съответствие

- Постигане на 100% съответствие с приложимото национално и европейско законодателство в областта на защитата на данните (например GDPR, AI Act) във всички публични институции, които обработват лични данни, като това се удостоверява чрез годишни правни прегледи.



- Утвърждаване и прилагане на вътрешните политики и стандарти за управление на данните в поне 90% от институциите, попадащи в обхвата на НРУД.
- Провеждане на задължително обучение относно принципите на управление на данните и правните задължения за 100% от служителите на определените длъжности, свързани с данни, като поне 80% от тях трябва да получат сертификат или да преминат оценяване в рамките на една година.
- Поддържане на централизирано хранилище/архив с документация, свързана с управлението на данни, включително политики, определения за роли, информация от обучения и резултати от одити, които да са достъпни за оторизираните надзорни органи и да се актуализират ежегодно.
- Ежегодно провеждане на независими одити за съответствие в поне 50% от институциите, като от всички одитирани институции се изисква да приложат мерки за разрешаване на несъответствията в рамките на три месеца след констатациите.

1.5 Елементи на категорията ИНСТИТУЦИИ



Фигура 2. Елементи на категорията ИНСТИТУЦИИ

1.5.1. Стратегия

Описание

Стратегическият елемент на НРУД очертава визията, целите и плановите, свързани с управлението на данните като стратегически публичен актив. Този



елемент гарантира, че управлението на данните е съгласувано с мисията и целите на публичната организация, като насърчава култура на вземане на решения, основани на данни, както и сътрудничество между публичния и частния сектор за използване на данните в обществен интерес.

Обхват

- Приемане на национално одобрена стратегия за управление на данните, съдържаща 3–5 измерими цели, които подкрепят пряко националните приоритети за развитие. Следва да се посочи ясно точно кои цели отговарят на националните приоритети за развитие.
- Сформиране на мултисекторен съвет за управление на данните, представляващ всички активни групи заинтересовани страни (администрацията, частния сектор, академичните среди, неправителствените организации), който да заседава веднъж на тримесечие, за да координира действията и осигури съгласуваност.
- Всяка ключова институция следва да назначи един координатор на пълен работен ден и да заложи целеви ежегоден бюджетен разход за поддържане на основните функции за управление на данните, като се проучат възможности за съгласуваност с институционалната рамка по Закона за достъп до обществена информация, съответно длъжностните лица, свързани с отворени данни.
- Привеждане на стратегията в съответствие с настоящата правна рамки и приложим международно признат стандарт, за да се гарантира съгласуваност, съответствие и оперативна съвместимост.
- Въвеждане на процес за управление на ефективността с приложими стратегически ключови показатели за изпълнение (КПИ) с ясна документация и методология, който да се преглежда периодично и да се споделя със заинтересованите страни, с цел поддържане на прозрачността и фокуса.
- Провеждане на оценки на готовността за промяна в поне три водещи агенции и на структурирани въвеждащи сесии с обхват от най-малко 50% от ангажирания персонал, за да се подготвят за прехода.



- Провеждане на две или повече обществени събития годишно, с цел да се демонстрира стойността на данните чрез реални примери за постигнато въздействие в областта на данните и за сътрудничество между публичния и частния сектор.
- Осведоменост и обучение: обхващане на поне 100 държавни служители годишно с персонализирано обучение за управлението на данни, защитата на данни и етичното им използване.
- Механизъм за активно подобрене: определяне на двугодишен цикъл за преглед и усъвършенстване на стратегия за цифрова трансформация на република България 2026-2030 г, в частта касаеща данните и включване на нови инструменти, анализи и иновации на местно ниво.

1.5.2. Ангажимент на високо ниво

Описание

Ангажиментът на високо ниво в НРУД включва осигуряване и поддържане на ангажираност и подкрепа на високо ниво от ключови ръководители/заинтересовани страни от публичния сектор. Такива отговорни лица на високо ниво подкрепят инициативи за управление на данните, осигуряват съгласуваност с организационните цели и предоставят необходимите ресурси и правомощия за прилагане на устойчиви, гъвкави и оперативно съвместими практики за управление на данните.

Обхват

- Осигуряване на видима подкрепа от висши ръководители или политически лидери, отразена в официални мандати или публични декларации и изявления в подкрепа на управлението на данните.
- Осигуряване на основни финансови, човешки и технологични ресурси чрез годишни цикли на планиране, при гарантирана минимална устойчивост на дейностите по управление на данни благодарение на ангажимента на високо ниво



- Представяне на приоритетите, свързани с управление на данните на поне три водещи публични форуми/платформи годишно - като например национални форуми, министерски речи или междусекторни кръгли маси.
- Обмисляне на учредяването на национална награда за управлението на данни, която да засили политическата видимост на темата и да ангажира поширок кръг заинтересовани страни.
- Демонстриране на съгласуваност чрез включване на целите за управление на данните в национални или организационни стратегически документи и секторни планове за действие.
- Дефиниране на ролите и отговорностите на спонсорите в официалните рамки за управление с механизми за проследяване на ангажимента и изпълнението.
- Създаване на обединение от различни групи заинтересовани страни, които активно допринасят за оформянето и изпълнението на инициативи за управление на данните.
- Използване на позициите на отговорни лица на високо ниво за подкрепа на разработването или усъвършенстването на поне една политика или регламент, който насърчава отговорното управление на данните
- Поддържане на ангажираността чрез редовни комуникационни кампании, брифинги за отговорните лица на високо ниво и споделяне на реални истории и примери, които подчертават напредъка и въздействието.

1.5.3. Организация

Описание

Организационният елемент на НРУД включва структуриране на роли, отговорности и процеси, с цел ефективно прилагане на управлението на данните. Включва дефиниране на управленски органи, ясно разпределение на роли и въвеждане на механизми за заместване и споделяне на знания, така че да се избегнат проблеми с капацитета (от типа single point of failure) и да се гарантира устойчивост и надеждност на дейностите.



Обхват

- Създаване на специализирани органи за управление, например национален главен служител по данните (Chief Data Officer), съвет за управление на данните (Data Governance Board) и работни групи, с официални мандати и редовна дейност.
- Ясно определяне и документиране на ролите – например отговорници за данни (data stewards), собственици (owners) и ползватели (users) – с осигуряване на регулаторно съответствие (например, с АУД на ЕС) и разпределяне на отговорността в рамките на официалните длъжностни характеристики или мандати.
- Поддържане на документирана структура, която подпомага управлението на данните в различните отдели, с ясни правила за отчетност и механизми за координация.
- Отразяване на всички структурни промени и на промените, свързани с ролите в актуализираните правни инструменти, вътрешни разпоредби или оперативни процедури.
- Въвеждане на програми за споделяне на знания за критични задачи, свързани с данни (например въвеждане и валидиране), като се гарантира, че всяка ключова функция следва да може да се изпълнява от поне двама души.
- Създаване на структурирани комуникационни платформи – като например срещи на работни групи, вътрешни портали или списъци за изпращане на комуникация – с цел да се даде възможност за редовни актуализации и съвместен обмен.
- Разработване на ключови показатели за изпълнение (КПИ) за оценка на ефективността на управленските структури и изпълнението на ролите, като прегледите се извършват поне веднъж годишно.
- Насърчаване на култура на непрекъснато усъвършенстване чрез използване на обратна връзка и оценки на ефективността с цел прецизиране на организационния дизайн и ролите.



1.5.4. Отчетност

Описание

Компонентът за отчетност на НРУД гарантира, че всички заинтересовани страни са добре запознати със своите роли в управлението на данните и носят отговорност за тяхното изпълнение. Това включва установяване на ясни линии на отчетност и правомощия, определяне на очаквания и прилагане на механизми за мониторинг и контрол на спазването на политиките и практиките за управление на данните.

Обхват

- Определяне и публикуване на RACI матрица (Responsible – Изпълнител, Accountable – Отговорен за резултата, Consulted – Консултиран, Informed – Уведомен), която обхваща основните роли, свързани с данните като отговорници за данни (stewards), попечители (custodians), собственици (owners) и ползватели (users) в поне три големи институции през първата година от прилагането.
- Разработване и разпространение на основни насоки за управление на данните, които съдържат минималните стандарти и очакваните практики, които да са достъпни до всички служители, чиито роли са свързани с данни.
- Въвеждане на вътрешно отчитане на напредъка в управлението на данните всяка година, като отчетите се споделят между отделите и с висшето ръководство.
- Провеждане на годишен одит или оценки за установяване на съответствието с основните политики за данните, като се използва подход, базиран на контролни списъци, за да се намалят необходимите ресурси. Въвеждане на основна рамка, която определя както последиците при неспазване на политиките за управление на данни (например писмени предупреждения), така и механизмите за признание при добро изпълнение (например сертификати или публично отбелязване на добри практики).



- Създаване на лесни и достъпни механизми за обратна връзка, като например анонимни формуляри или редовни срещи със служителите за събиране на предложения и идентифициране на проблеми, свързани с отчетността.
- Идентифициране и описване на основните рискове, свързани с данните, във всяка институция и въвеждане на поне една мярка за отчетност за смекчаване на всеки идентифициран риск.
- Ежегоден преглед на практиките за отчетност и актуализиране на инструментите или рамките на базата на резултатите от одита, обратната връзка, получена от служителите и институционалните потребности.

1.5.5. Подкрепа и застъпничество за използване на данните

Описание

Подкрепата и застъпничеството за използването за данните се фокусират върху утвърждаване на стойността, осведомеността и отговорното използване на данни в рамките на институциите, чрез ангажиране, обучение и овластяване на заинтересованите страни. Този елемент цели да изгради култура, ориентирана към данните, както и да гарантира, че принципите за управление на данните се разбират и възприемат от всички служители. Застъпничеството за данните играе ключова роля в прехода от формулирането на политики по управление на данните към тяхното прилагане в ежедневната практика, като утвърждава възприятието за данните като обществен актив.

Обхват

- Всяка година поне двама висши ръководители изразяват подкрепа за вземането на решения, базирани на данни, чрез изказвания в медиите.
- Популяризиране на поне три значими инициативи, свързани с данни, годишно чрез популярни медии или обществени форуми, с цел да се покаже тяхната стойност и да се насърчи прилагането им от други.
- Организиране на поне две събития годишно (например форуми, дни на отворените врати или тематични седмици), с цел популяризиране ролята на данните за създаване на обществена стойност и иновации.



- Идентифициране и овластяване на застъпници за данни в поне три отдела, с цел насърчаване на добрите практики за данни и стимулиране на ангажираността на колегите им.
- Поддържане на постоянни пространства за сътрудничество (виртуални или присъствени), където отговорниците за данни (data stewards), анализаторите и потребителите могат да обменят предизвикателства, идеи и решения.
- Включване на кратки съобщения в месечната или тримесечната вътрешна комуникация с цел утвърждаване на прозрачността относно използването на данните – как се използват, защитават и усъвършенстват.
- Използване на инструменти за обратна връзка (като анкети или фокус групи) два пъти годишно, за събиране на информация относно нуждите, възприятията и пречките, които служителите срещат при използването на данни.

1.5.6. Стратегия за уменията

Описание

Стратегията за умения в НРУД има за цел да развие и поддържа компетенциите, необходими за ефективното управление на данните. Този елемент се фокусира върху идентифицирането, усъвършенстването и надграждането на уменията, свързани с данните, в цялата организация. Чрез установяване на ясни механизми за развитие на уменията, стратегията гарантира, че служителите са подготвени да управляват, анализират и предпазват информационните активи, като така се изгражда култура на цифрова грамотност и учене през целия живот.

Обхват

- Оценка на основните умения поне на всеки две години за ключови роли (например служители по данните (data officers), отговорници (stewards), собственици и служители по защита на данните), с цел идентифициране на нуждите от обучение.



- Предоставяне на структурирано обучение за поне три приоритетни роли годишно, обхващащо теми като качество на данните, метаданни, защита и етично използване на данни.
- Партньорство с поне две местни или регионални институции, които предлагат обучение, с цел предоставяне на подходящи курсове или сертификати в областта на управлението на данни.
- Насърчаване на продължаващо обучение чрез предлагане на достъп до семинари, кратки курсове или платформи за обучение за служителите, работещи с данни в различните институции.
- Организиране на поне две вътрешни сесии за споделяне на знания годишно (например срещи с общността или прегледи на казуси), с цел да се насърчи взаимното обучение и ученето между колеги.
- Подпомагане на участието в поне един външен форум, общност за обмяна на практики или конференция годишно за специалистите по управление на данни.
- Преглед и актуализация на плана за развитие на уменията на всеки две години, в съответствие с новите технологии, промени в политиките и организационните нужди.

2. КАТЕГОРИЯ ПОЛИТИКИ

2.1 Описание

Категорията ПОЛИТИКИ въвежда официални насоки, стандарти и политики, които ръководят събирането, съхранението, прехвърлянето, управлението и използването на данни в публичната администрация. Тя определя принципи и стандарти за съхранение на данни, управление на метаданни, качество на данните и прозрачност на алгоритмите, с цел да се гарантира интегритетът и поверителността на данните, както и спазването на законовите и регулаторните изисквания. Ефективните политики за данни свеждат до минимум рисковете, свързани с нарушения на сигурността на данните, неоторизиран достъп и загуба на



данни, като същевременно насърчават етичното и прозрачно използване на данните.

2.2 Цел

Целта на категорията ПОЛИТИКИ е да осигури структуриран подход към управлението на данните чрез определяне на ясни правила и стандарти за управление на данни в рамките на публичната администрация. Тези политики гарантират, че данните се обработват с точност, сигурност и висока степен на надеждност, като по този начин се подпомага ефективното вземане на решения и спазването на нормативните изисквания. Чрез установяване на устойчиви стандарти за съхранение, защита и качество на данните, тази категория има за цел да намали грешките, да предотврати неоторизиран достъп и да насърчи отчетността. Категорията също така стимулира прозрачността и общественото доверие, като гарантира, че данните се използват етично и отговорно, подпомагайки ефективността на управлението.

2.3 Рискове

Съществуват рискове, които могат да отслабят ефективността на политиките за управление на данните, ако не бъдат адресирани своевременно и проактивно. Липсата на ангажираност при разработването и прилагането на политиките може да доведе до слабости в реализацията и контрола, което ограничава нивото на спазването им в различните звена на организацията. Непоследователното прилагане в различните отдели може допълнително да навреди на ефективността на политиките, създавайки неравномерни практики и асиметрии по отношение на управлението и сигурността на данните.

Слабите политики могат също да допринесат за проблеми с качеството на данните, което да доведе до неточни или ненадеждни данни, използвани при вземането на решения и предоставянето на публични услуги. Недостатъчните мерки за защита на данните увеличават риска от нарушения на сигурността и неоторизиран достъп, излагайки организациите на репутационни и правни последици. Недостатъчното финансиране може допълнително да ограничи



разработването и прилагането на всеобхватни политики за данните, възпрепятствайки тяхната ефективност.

Допълнително предизвикателство представлява необходимостта от съответствие с международни правила за трансфер на данни. Несъответствието с тях може да доведе до правни спорове и уязвимости в сигурността. Липсата на прозрачност и стандарти при използването на алгоритми създава риск от пристрастия/отклонения и несправедливи резултати при автоматизираните решения. Също така, липсата на съгласуваност на политиките с цялостните стратегическите цели може да възпрепятства управлението на данните и да попречи на организациите да използват пълноценно данните като стратегически актив. Ефективното справяне с тези рискове изисква редовна оценка на политиките, активно включване на заинтересованите страни и съобразяване с регулаторните и технологични промени.

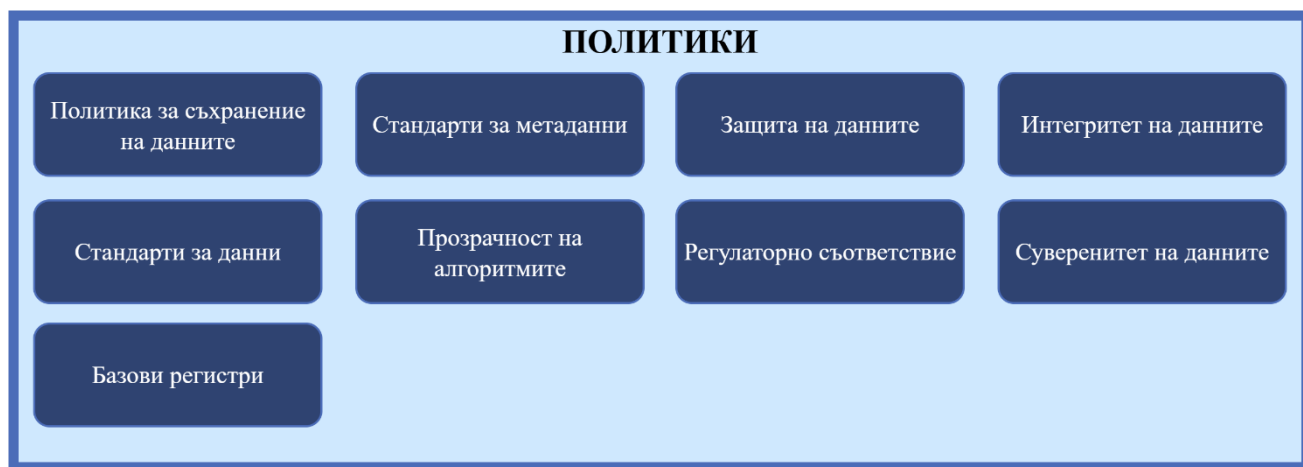
2.4 Изисквания за съответствие

- Осигуряване на съответствие с националните и международните закони и разпоредби за защита и за управление на данните.
- Определяне на ролите и отговорностите за управление на данните, включително собственост върху данните, разпореждане с данните и юрисдикция.
- Използване на одобрени механизми за трансгранично прехвърляне на данни, с цел спазване на международните споразумения за защита на данните.
- Въвеждане на стандарти за външни партньори и доставчици, с цел да се гарантира, че те спазват едни и същи изисквания за управление и сигурност на данните.
- Осигуряване на програми за обучение на служителите във връзка с политиките, стандартите и насоките, свързани с управлението на данни.
- Провеждане на системни одити и прегледи на политиките, с цел да се идентифицират пропуски и да се гарантира непрекъснато усъвършенстване.



- Прилагане на надеждни механизми за мониторинг и отчетност, с цел да се проследява спазването на политиките за данни и регулаторните изисквания.
- Поддържане на подробна документация за всички политики, процеси и промени, свързани с данните, за да се подкрепи прозрачността и отчетността.
- Разработване и въвеждане в сила на планове за корективни действия/мерки въз основа на констатациите от одити и мониторинг, с цел преодоляване на несъответствията и повишаване ефективността на политиките.
- Гарантиране на прозрачност при използването на алгоритми за обработка на данни чрез регулярни прегледи за справедливост и съответствие с етичните стандарти.

2.5 Елементи на категорията ПОЛИТИКИ



Фигура 3. Елементи на категория ПОЛИТИКИ

2.5.1 Политика за съхранение на данните

Описание

Политиката за съхранение на данните определя насоки за това колко дълго следва да се съхраняват, архивират и евентуално заличават данните, като гарантира ефективно управление и спазване на законовите и регулаторни изисквания. Тази



политика спомага за поддържане на качеството и релевантността на данните, като запазва само необходимата информация и премахва остарелите данни. Прилагането на строга политика за съхранение на данните позволява на публичната администрация да намали разходите за съхранение, да подобри сигурността на данните и да оптимизира процесите на управление на данните, като гарантира, че те са достъпни само докато са полезни или докато се изискват от закона.

Обхват

- Създаване на национална или институционална схема за класификация на данните с поне три категории (например публични, вътрешни и чувствителни данни), всяка с дефинирани периоди за съхранение.
- Публикуване на график за съхранение на данните, който определя колко дълго се съхраняват, архивират и кога се изтриват различните типове и набори данни, съобразен с правните изисквания и оперативните нужди.
- Прилагане на поне един автоматизиран или полуавтоматизиран процес за архивиране или изтриване на данни съгласно определения график за съхранение.
- Осигуряване на достъп до архивираните данни само от оторизирани служители, с документиран нива на достъп.
- Използване на базови мерки за сигурност (например криптиране или защита с парола), с цел защита на чувствителни данни при съхранение и пренос.
- Демонстриране, че правилата за съхранение са в съответствие с поне един приложим нормативен акт или разпоредба (например ОРЗД, национален закон за защита на данните), които са преглеждани ежегодно за актуализации.
- Провеждане на вътрешни проверки или одити поне веднъж годишно, за потвърждаване на спазването на политиката за съхранение на данни, като се обмисли и провеждането на външни одити.
- Преместване на неактивните данни в нискобюджетно и сигурно дългосрочно хранилище/архив в рамките на шест месеца след



установяване на неактивността им, като се гарантира наличието на процедури за възстановяване.

- Безопасно и трайно изтриване на остарели данни в съответствие с предвидените срокове, като се съхраняват логове/журнали за изтриването за целите на отчетността.
- Актуализиране на графици и практиките за съхранение на данни на всеки две години, с цел отразяване на актуалните правни, технически или организационни промени.
- Запазване на резервни копия на критични данни и ежегодно тестване на процедурите за възстановяване, с цел предотвратяване на загуба на данни.
- Осигуряване на регулярно въвеждащо или опреснително обучение по политиките за съхранение на данни за 100% от служителите с отговорности в тази област, поне веднъж на всеки две години.

2.5.2 Стандарти за метаданни

Описание

Стандартите за метаданни определят как трябва да бъдат структурирани, описани и управлявани метаданните, за да се осигурят последователност, яснота и оперативна съвместимост в рамките на публичната администрация. Тези стандарти спомагат за поддържане на унифицирани методи за документиране на данните, което позволява по-ефективно откриване, споделяне, оперативна съвместимост, интеграция и управление на качеството на данните. Прилагането на такива стандарти гарантира, че данните са разбираеми и използваеми от всички заинтересовани страни.

Обхват

- Приемане на поне три международно признати стандарта за метаданни (например, Приложния профил на каталога на данни за Европейския портал за данни (DCAT-AP), ISO 19115, Dublin Core, и др.) и гарантиране, че те се прилагат за 100% от новите набори от данни, които се създават, публикуват или споделят.



- Определяне на задължителни, препоръчителни и незадължителни полета за метаданни за поне три основни категории данни, ясно документиран и достъпен за всички, които публикуват данни.
- Гарантиране, че полетата за метаданни са дефинирани според последователни синтактични правила, включително конвенции за именуване, типове данни и разрешени стойности, чрез използването на контролирани речници, където е приложимо.
- Въвеждане на структура на метаданните, която позволява свързване между съответни набори от данни и поддържа йерархия (например колекции, подколекции и теми).
- Изискване за поне пет широко използвани набори от данни да включват проследимост, което включва произход на данните, трансформации и системни движения.
- Задължително използване на контролирани речници и таксономии (национални или специфични за дадената област), с цел да се гарантира яснота и съгласуваност между различните набори от данни.
- Осигуряване на оперативна съвместимост на метаданните чрез съпоставяне на националните практики с поне един международен стандарт, за да се подпомогне трансграничния и междуетовен обмен на данни.
- Предоставяне на шаблони или таблици за преобразуване за интегриране на външни данни във вътрешни структури от метаданни с минимална ръчна обработка.
- Поддържане на централизирано хранилище за метаданни с модели, примери и насоки за приложение, които се използват в държавните институции.
- Определяне на ясни роли за отговорниците за данни и провеждане на годишни прегледи на качеството на извадка от метаданни, с цел гарантиране на съответствие.



- Комуникиране на всички актуализации на изискванията за метаданни чрез официални канали и отразяване на промените в инструментите, шаблоните и порталите в срок до шест месеца.

2.5.3 Защита на данните

Описание

Защитата на данните представлява рамка, която гарантира сигурността на чувствителните и регулирани данни, като предотвратява неоторизиран достъп, загуба на данни и нарушения/пробиви. Тя установява насоки за защита на поверителната информация, като привежда практиките за обработка на данни в съответствие с правните и регулаторните изисквания. Прилагането на политика за защита на данните помага на публичната администрация в опазването на чувствителни данни както на публичните институции, така и на гражданите, като същевременно изгражда обществено доверие и гарантира съответствие с регулаторните изисквания. Това допринася за защитата на репутацията на институциите и за осигуряване на поверителността на информацията. Предвид високото ниво на чувствителност и изискванията за дългосрочно съхранение на данни, от съществено значение е постигането на балансиран подход, който съчетава защитата на легитимни интереси – като лични данни, чувствителна търговска информация и данни, свързани със сигурността – с необходимостта от съответствие с националното законодателство и регулациите относно достъпа до информация.

Обхват

- Гарантиране, че 100% от системите, обработващи лични или поверителни данни, прилагат контрол на достъпа на базата на роли, съобразен с утвърдени политики за оторизация.
- Изискване за всички чувствителни данни да бъдат защитени чрез одобрени мерки за сигурност, като криптиране и/или маскиране, прилагани последователно при съхранението и трансфера на данните.
- Задължително провеждане на редовни вътрешни одити (например веднъж в годината) за проверка на спазването на националните и



международните разпоредби за защита на данните, с документираните резултати и последващи коригиращи действия.

- Следва да се гарантира, че всички публични институции разполагат с документираните и тествани процедури за откриване, докладване и реакция при нарушения на сигурността на данните, съобразени със законовите срокове.
- Изискване потвърдените инциденти, свързани със защитата на данните, да бъдат разследвани, разрешени и докладвани съгласно одобрените протоколи за реагиране при инциденти, като се минимизира излагането на риск и въздействието.
- Поддържане на непрекъсваемост на дейността, чрез въвеждане на изискването за наличие на тествани планове за възстановяване и наличие на сигурни резервни копия за всички критични набори от данни, с обективно време за възстановяване (Recovery Time Objective), определени в политиката.
- Задължение 100% от служителите, които имат достъп до чувствителни данни, да преминават обучение за защита на данните поне веднъж на всеки две години, с актуализирано съдържание, отразяващо регулаторни промени или промени в политиките.
- Привеждане на политиките за защита на данните в съответствие с развиващите се правни рамки (например GDPR и националните закони за поверителност), с преглед поне веднъж на всеки две години, за да се осигури съответствие.

2.5.4 Интегритет на данните

Описание

Политиката за интегритет на данните гарантира, че данните от публичния сектор остават пълни, точни и непроменени през целия си жизнен цикъл. Тя определя стандарти и контролни механизми, необходими за защита на данните от неоторизирана промяна, изтриване или повреда. Поддържането на интегритета на данните е от съществено значение за изграждането на обществено доверие, за



вземане на решения, основани на доказателства, и за съответствие с регулаторните изисквания. Чрез прилагането на стабилна политика за интегритета на данните, публичните администрации могат да гарантират, че данните остават надеждни и достоверни, което позволява ефективно предоставяне на услуги и прозрачно управление.

Обхват

- Ограничаване на правата за промяна на данни до определени служители, като разрешенията се дават и преглеждат ежегодно за всички системи от критична важност.
- Гарантиране на наличието на активни одитни следи в домейни с чувствителни данни, които да записват кой, кога и защо е променял данните. Лог файловете и файловете от журналът на промените да се съхраняват минимум 12 месеца.
- Провеждане на проверки за интегритет на приоритетните набори от данни (минимум веднъж на тримесечие), като се проверява точността, пълнотата и съгласуваността спрямо изходните системи.
- Въвеждане на опростен процес за откриване на аномалии (ръчен или автоматизиран) за критични масиви от данни, с цел идентифициране на необичайни промени или несъответствия в реално или в почти реално време.
- Поддържане и тестване на процедурите за възстановяване на данни за всички критично важни системи поне веднъж годишно, като се гарантира пълно възстановяване в рамките на 48 часа. Установяване на минимални изисквания относно честотата на архивиране на критични набори от данни (например ежедневно или веднъж седмично), със защитено съхранение на лог файловете и файловете от журналът на промените за потвърждение.
- Провеждане, веднъж на всеки две години, на целево обучение относно ролите и рисковете, свързани с интегритета на данните за поне 80% от служителите, които се занимават с обработване на данни, като



съдържанието на обучението се актуализира след съществени промени в политиките или в системата.

- Извършване на периодично съгласуване на данни между системите (минимум веднъж годишно), с цел да се гарантира на последователност и съответствие на споделените набори от данни между различните платформи.

2.5.5 Стандарти за данни

Описание

Стандартите за данни определят правилата и критериите, които гарантират качеството, съгласуваността и формата на данните в дадена област. Те предоставят структурирана рамка за управление на данни, давайки възможност за унифициране, общо разбиране и оперативна съвместимост между различните системи и процеси. Чрез приемането и прилагането на стандарти за данни, организациите от публичния сектор могат да подобрят вземането на решения и интеграцията на данните, и да осигурят съответствие с регулаторните изисквания. Последователното прилагане на стандартите за данни подкрепя прозрачността, отчетността и ефективността на обществените услуги, като същевременно защитава качеството и сигурността на данните.

Обхват

- Осигуряване поне 75% от публикуваните набори от данни да отговарят на стандартната структура, в т.ч. имена на полета, типове данни, формати и конвенции за именуване, която е документирана в публичните метаданни.
- Стандартизиране на шаблоните за отчетност във всички институции, които създават данни за публично ползване, с цел да се осигури съпоставимост и лесно разбиране.
- Дефиниране и въвеждане на стандартни процедури за интеграция и обмен на данни между поне три основни системи, което ще осигури безпроблемна оперативна съвместимост.



- Създаване на протоколи за свързване на данни и управление на съгласието, в случаите, в които данните се споделят между различни отдели или юрисдикции, с правни и етични гаранции.
- Следва да се гарантира, че всички анонимизирани набори от данни, използвани за анализ или споделяне, следват определен международен или одобрен от сектора стандарт за деидентификация.
- Публикуване на ясни насоки за етичното използване на данни, включително правила за съгласие, прозрачност и отчетност, които трябва да се спазват във всички инициативи, свързани с публични данни.
- Въвеждане на изискване за използването на уникални идентификатори и стандартизирани кодове (например гео-кодове, идентификатори на организации) в наборите от данни, споделяни между институции или трансгранично, за осигуряване на проследимост и съответствие.
- Преглед и актуализация на документацията за стандартите за данни на всеки две години, като се отчитат нововъзникващи практики, международни стандарти и обратна връзка от заинтересованите страни.

2.5.6 Прозрачност на алгоритмите

Описание

Прозрачността на алгоритмите установява насоки, които гарантират, че използването на алгоритми при вземането на решения в държавната администрация е отговорно, прозрачно и етично. Тя изисква оповестяване на начина, по който се разработват алгоритмите, какви данни използват и какви критерии прилагат при вземането на решения. Тази политика има за цел да оцени и ограничи системните рискове, като например наличие на пристрастия и неволни последици, свързани с информационните системи. Като прави тези процеси видими и разбираеми, политиката насърчава справедливостта, защитава правата на гражданите и изгражда обществено доверие в автоматизираните публични услуги.

Обхват



- Публично оповестяване на източниците на данни, типовете модели и методологиите за обучение, използвани в поне 80% от информационните системи, управлявани от държавната администрация.
- Гарантиране, че всички алгоритми, обработващи лични или чувствителни данни, включват документирана проследимост на данните и оценки за качеството им.
- Извършване на оценки на риска за 100% от информационните системи преди внедряването им, включително оценка на потенциални пристрастия, дискриминация или вреди.
- Прилагане на поне една техника или предпазна мярка за ограничаване на пристрастията за всеки алгоритъм с висок риск, с налична документация за преглед.
- Извършване на вътрешни проверки или независими одити на работата на алгоритмите и справедливостта им поне веднъж на всеки две години за критичните системи в обществените услуги.
- Осигуряване на цифров или физически канал, чрез който гражданите могат да подават обратна връзка или сигнали относно решения, базирани на алгоритми, с максимален срок за отговор до 30 дни.
- Публикуване на поне един публично достъпен ресурс годишно (например табло, доклад или разяснителен материал), с цел да се повиши осведомеността относно използването на алгоритми и да се подпомогне постигането на обществено разбиране.
- Преглед на информационните системи, използвани в обществените услуги, за съответствие с насоките за прозрачност и политиките за управление на данните поне веднъж на всеки 24 месеца.

2.5.7 Регулаторно съответствие

Описание

В контекста на управлението на данни регулаторно съответствие означава въвеждане на необходимите за рамката изисквания на различни равнища в системата от правно обвързващи документи, както и извършване на необходимите



промени там, където съществуващи нормативни актове или вътрешни правила противоречат на елементите на политиката за управление на данните. Практиките, процесите, политиките и техническите инструменти за управление на данните трябва да са в съответствие с местното, националното и европейското законодателство, поради което е необходим процес на съгласуване винаги когато се въвеждат нови политики и процеси или се възлага разработката на нови информационни системи и други инструменти.

Обхват

- Определяне и публикуване на правно признати термини за поне пет основни понятия (например качество на данните, метаданни, собственост, отговорност за данни (stewardship) и жизнен цикъл) в официални регулаторни документи или в документи с политики, като например стратегии.
- Въвеждане на законово определяне на ролите при управлението на данните, като например служители, обработващи данните (processors), отговорници за данни (stewards) и служители по защита на данните (protection officers) в основните публични институции, обработващи чувствителни или споделени данни.
- Установяване на правни разпоредби, позволяващи структурни промени, като например създаването на централен орган за управление на данните или механизми за междуведомствена координация, където е необходимо.
- Въвеждане и публикуване на правно приложими срокове за регулаторни реформи или институционални адаптации, свързани с управлението на данните.
- Задължително преглеждане на всички нови разпоредби, свързани с данните, с цел проверка за съгласуваност и гарантиране на съответствие с националната стратегия за управление на данните и с международните задължения.
- Въвеждане на правна уредба, която да изисква периодичен преглед и актуализация на рамката за управление на данните поне на всеки пет



години, с цел да се адаптира към технологичните развития и промените в политиките.

- Въвеждане на правни механизми за контрол на изпълнението и мониторинг на съответствието, които включват санкции, задължения за докладване и процедури за обезщетение при нарушения на отговорностите, свързани с управление на данните.

2.5.8 Суверенитет на данните

Описание

Суверенитетът на данните се отнася до две свързани, но независими концепции, които трябва да бъдат част от всяка рамка за управление на данните. В общ смисъл суверенитетът на данните визира запазването на контрол върху притежаваните данни. Контролът в този контекст означава, че притежателите на данни разполагат със средства да гарантират, че техните данни се споделят, използват и управляват съобразно собствените им политики, нужди и правни задължения. От една страна, това е свързано с физическия и юридическия контрол върху данните, т.е. с принципа, че данните, които се събират, съхраняват или обработват в дадена държава, се регулират от законите и разпоредбите на тази държава. Това означава, че всички организации от публичния сектор трябва да управляват данните по начини, които отговарят на националните правни стандарти, независимо от това къде или как се осъществява достъп до тях. Този подход гарантира, че чувствителната и личната информация на гражданите остава под националната юрисдикция, като по този начин се повишава поверителността, сигурността и отчетността.

От друга страна, суверенитетът на данните се отнася до всякакви правни или технически средства, които гарантират, че всички данни, споделяни с втори или трети страни, се използват повторно само до степента, определена от политиката за лицензиране и правните задължения, които собственикът има. Например, данни на индивидуално ниво, които попадат в обхвата на личните данни съгласно GDPR, могат да се споделят само по начини, които гарантират спазването на защитата на личните данни (например само в алгоритмична среда, без директен



достъп до данните, анонимизирани или агрегирани). В друг пример, когато дадена институция допуска еднократна употреба на свои данни за целите на изследователски проект, тя следва да определи чрез споразумение за неразкриване на информация или чрез други технологични средства (например, пространство от данни), че другата страна няма право да копира или разпространява данните и е обвързана със същите правни задължения като собственика на данните.

Суверенитетът на данните защитава правата на гражданите и поддържа национален контрол върху критична информация, което е от съществено значение за надеждното и сигурно управление на данните във всички публични сектори.

Обхват

- Въвеждане на законови изисквания, според които 100% от личните и чувствителни данни, съхранявани от държавната администрация, се съхраняват и обработват в рамките на националните граници, освен ако това изискване не е изрично отменено по закон.
- Гарантиране, че всички договори за хостинг на данни с трети страни включват обвързващи клаузи, които изискват спазване на националното законодателство в областта на данните.
- Провеждане на ежегодни прегледи за съответствие за всички държавни облачни услуги и услуги, свързани с данни, с цел да се провери степента на спазване на правилата за суверенитет и политиките за съхранение на данните.
- Създаване на механизъм за предварително одобрение при трансгранични потоци от данни, с ясно документиране и мониторинг на всяко изключение и свързаните рискове.
- Изискване всички публични институции, използващи облачни услуги, да избират доставчици с центрове за данни на национална територия или сертифицирани опции за „суверенен облак“.
- Въвеждане на изискване 100% от новите системи за данни, въведени в публичните институции, да отговарят на юрисдикционните изисквания относно мястото на постоянно пребиваване на данните от самото начало.



- Публикуване на годишен доклад относно спазване на суверенитета на данните, който обобщава рисковете, предоставените изключения и предприетите действия за изпълнение от страна на публичните институции.

2.5.9 Базови регистри

Описание

Базовият регистър е надежден източник на достоверни данни с високо качество, като например данни за хора, фирми, превозни средства, лицензи, сгради, места и пътища. Информацията в един базов регистър трябва да бъде с толкова високо качество и надеждност, че публичните органи да могат да я използват уверено без необходимост от допълнителна проверка, което да позволява безпроблемно цифрово повторно използване в различни приложения. Това насърчава ефективността, намалява административната тежест за гражданите чрез премахване на необходимостта от повторно подаване на данните и подпомага ефективното предоставяне на обществени услуги.

Обхват

- Официално определяне и публикуване на списък с одобрени базови регистри на национално ниво, които обхващат поне пет основни области, например: население, адресна регистрация, собственост, бизнеси и превозни средства.
- Въвеждане на контрол на достъпа и проверки за съответствие, които да гарантират, че всички базови регистри спазват националните закони за защита на данните и на поверителността и разполагат с механизми за докладване на инциденти.
- Въвеждане на синхронизация в реално време или на периодична синхронизация между базовите регистри и системите, които ги използват, като интеграцията се тества поне два пъти годишно.
- Дефиниране и публикуване на ясни условия за използване на всеки базов регистър, включително разрешени видове употреба, ограничения и протоколи за достъп за оторизирани лица.



- Гарантиране, че 100% от оторизираните публични институции имат достъп до данните от базовия регистър чрез стандартизирани приложно-програмни интерфейси или услуги за данни, като по този начин се намалява дублирането на събиране на данните.
- Установяване на цикли на актуализация на данните (например ежедневно, веднъж седмично или веднъж месечно) и на процедури за валидиране, които да важат за всички базови регистри, като статусът на актуализациите е публично проследим.
- Предоставяне на годишни отчети за ефективността за всеки базов регистър, които включват статистика относно употребата, показатели за качество на данните и обратна връзка от потребителите.

3. КАТЕГОРИЯ ПРОЦЕСИ

3.1 Описание

Категорията ПРОЦЕСИ в НРУД се фокусира върху въвеждането и поддържането на стандартизирани процеси за управление на данните през целия им жизнен цикъл. Тя включва поддръжка на данни, управление на качеството, управление на инциденти и т.н., с цел да се гарантира последователност при обработката на данни. Тази категория е от решаващо значение за безпроблемното управление на данните, като осигурява структурата, необходима за изпълнение на политиките и гарантира, че данните се използват ефективно във всички национални институции. Посредством интеграцията на най-добри практики и непрекъснат мониторинг, тя има за цел да оптимизира процесите, свързани с управление на данните и да смекчи оперативните рискове.

3.2 Цел

Целта на категорията ПРОЦЕСИ е да осигури структуриран подход към управлението на операциите и дейностите с данни, като гарантира, че предварително определените и договорени принципи за управление на данните се прилагат последователно през целия им жизнен цикъл. Тя има за цел да стандартизира процеси като поддръжка на данни, управление на качеството,



реакция при инциденти и контрол на промените, с цел да се сведат до минимум рисковете, да се поддържа високо качество на данните и да се гарантира съответствие с регулаторните стандарти. Тази категория подкрепя създаването на прозрачно и ефективно управление на данните, като позволява по-добро вземане на решения, насърчава изграждането на доверие между заинтересованите страни и гарантира, че данните представляват надежден и сигурен актив за страната.

3.3 Рискове

Ефективните процеси за управление на данните разчитат на безпроблемна координация, последователен мониторинг и достатъчни ресурси. Липсата на координация между заинтересованите страни обаче може да доведе до фрагментиране на усилията, несъответствие в дейностите по управление на данните и неефективност в области като поддръжка на данни, контрол по прилагането на политики и управление на доверието. Липсата на мониторинг може да попречи на навременното идентифициране на проблеми с качеството на данните, на рискове за сигурността или на несъответствия, което оказва негативно въздействие върху ефективността на управлението на инциденти и контрола на промените. Освен това, ограниченията, свързани с ресурсите – финансови, технически или човешки – могат да възпрепятстват изпълнението и устойчивостта на инициативите за управление, включително управлението на жизнения цикъл на данните, откриването на данни и прилагането на политики.

Освен предизвикателствата, свързани с ресурсите и контрола, неоторизираните промени представляват риск за процесите на дефиниране на данните и управлението на доверието, което води до несъответствия и по-малка надеждност на данните. Загубата на данни по време на поддръжката може да възникне поради недостатъчни мерки за безопасност и да засегне критично важни процеси за управление на качеството на данните и на жизнения им цикъл. Неспазването на изискванията при въвеждането и координацията на политики могат да изложат организациите на правни рискове и да навредят на репутацията им. Съпротивата срещу промените от страна на ключови заинтересовани страни може да забави приемането на подобрени работни процеси за управление на



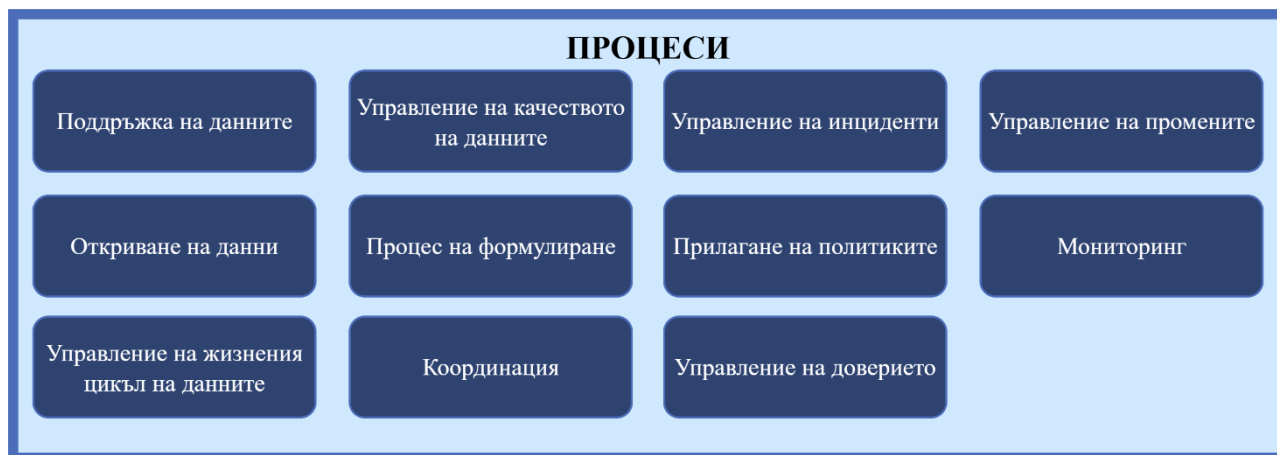
данните и механизми за мониторинг. За да се смекчат тези рискове и да се гарантира устойчивост и гъвкавост, публичните организации следва да инвестират в стабилни и постоянни контролни механизми, както и в структурирано управление на промените.

3.4 Изисквания за съответствие

- Осигуряване на продължаващо обучение за служителите, които участват в обработката на данни, с цел повишаване на осведомеността относно изискванията за съответствие и добрите практики.
- Гарантиране, че всички процеси отговарят на приложимите регулаторни актове и разпоредби в областта на защитата и поверителност на данните (например GDPR).
- Въвеждане и поддържане на практики за управление на качеството на данните, които са в съответствие с вътрешните и с международните стандарти за данни.
- Поддържане на подробни записи относно всички инциденти, включително предприетите действия и резултатите, с цел осигуряване на отчетност и прозрачност.
- Спазване на стандартизирани процедури за одобрение и документиране на промените, с цел да се гарантира надеждността на данните.
- Извършване на периодични одити на процесите, свързани с данни, с цел да се потвърди съответствието с вътрешните политики и нормативните изисквания.
- Въвеждане на механизми за непрекъснат мониторинг и докладване, с цел бързо откриване и разрешаване на проблеми с качеството или сигурността на данните.
- Поддържане на подробна документация относно всички процеси на управление на данни, за да се осигури проследимост и съответствие.
- Разработване и прилагане на коригиращи действия за отстраняване на всяко установено несъответствие или неефективност на процесите, с цел непрекъснато усъвършенстване.



3.5 Елементи на категорията ПРОЦЕСИ



Фигура 4. Елементи на категорията ПРОЦЕСИ

3.5.1 Поддръжка на данните

Описание

Поддръжката на данни обхваща непрекъснатия процес на управление и актуализиране на данните, с цел да се гарантира тяхната точност, последователност и надеждност. Това включва рутинни задачи като почистване на данни, актуализиране на записи, коригиране на грешки и гарантиране, че данните са актуални и приложими за нуждите на организацията. Ефективната поддръжка на данните подпомага информираното вземане

Обхват

- Спазване на документиран работни инструкции или процедури за работа от поне 95% от отговорниците и собствениците на данни, като тези документи се подлагат на преглед и актуализация поне веднъж годишно.
- Идентифициране и коригиране на неточности в данните или проблеми с формата в приоритетни набори от данни поне веднъж на всеки три



месеца, като процентът на грешки се документират и проследяват във времето.

- Поддържане на съответствие с националните стандарти за данни за поне 90% от структурираните набори от данни, което следва да се верифицира чрез рутинни проверки.
- Актуализиране на наборите от данни, чиято актуалност е от критично значение (например население, адреси, имоти), на регулярни интервали - ежедневно, ежеседмично или ежемесечно, в зависимост от оперативните нужди.
- Прилагане на правила за автоматизирано и/или ръчно валидиране за 100% от входящите потоци от данни преди интегрирането им в продукционна среда.
- Архивиране на остарели или рядко използвани данни съгласно графика за съхранение, като се гарантира, че поне 95% от архивираните данни могат да бъдат възстановени в рамките на 48 часа.
- Поддържане на качеството на метаданните за предварително определените приоритетни набори от данни, включително дата на последна актуализация, източник и собственост, които се преглеждат поне два пъти годишно.
- Документиране на произхода и трансформацията на всички критични набори от данни, с цел осигуряване на проследимост, като записите за проследимост на данните са достъпни за оторизирани потребители.

3.5.2 Управление на качеството на данните

Описание

Качеството на данните определя стандартите и практиките, които осигуряват пълнота, навременност, валидност, точност и съгласуваност на данните, управлявани от публичната администрация. Висококачествените данни подпомагат ефективното вземане на решения, подобряват общественото доверие и позволяват ефективно предоставяне на услуги, като гарантират, че информацията



е изчерпателна, надеждна и подходяща за целите, за които се използва. Управлението на качеството на данните включва систематични процеси и практики, за поддържане на точност, пълнота, надеждност и уместност на данните. Допълнителни насоки относно принципите и практиките за управление на качеството на данните, са представени в ръководството на ЕК – „Data.europa.eu Data Quality Guidelines“¹. Документът очертава основните измерения, методологии и най-добри практики за осигуряване на висококачествени данни в институциите от публичния сектор. Елементът, свързан с управление на качеството на данните, се фокусира върху прилагането на стандарти за качество на данните, наблюдението на показателите за качество на данните, идентифицирането и отстраняването на проблеми с данните и непрекъснатото им подобрене.

Обхват

- Установяване на правила и показатели за точност, пълнота, консистентност и навременност на данните (според стандартите на ISO 8000).
- Гарантиране, че 100% от критичните набори от данни включват документиран спецификации за качество, които са съобразени с оперативните и регулаторните изисквания.
- Създаване на критерии за качество на данните, съобразени с целите на организацията.
- Прилагане на правила за валидиране и бизнес проверки за поне три основни системи за данни, с цел да се осигури съответствие със стандартите за качество при въвеждане или обработка на данни.
- Провеждане на прегледи на качеството на ключови набори от данни поне два пъти годишно, при които се идентифицират и отстраняват пропуски или повтарящи се проблеми.
- Документиране на метаданните за всички публикувани набори от данни, включително дефиниции, източници и проследимост, с цел подпомагане на прозрачността и гарантиране на качеството на данните.

¹ <https://op.europa.eu/en/publication-detail/-/publication/023ce8e4-50c8-11ec-91ac-01aa75ed71a1>



- Установяване на ясни процедури за докладване и последващо разрешаване на проблеми с качеството на данните, с определени роли за отговорните служители и срокове.
- Въвеждане на механизъм за докладване на качеството на данните в поне три приоритетни области, с тримесечно актуализиране за проследяване на показатели и споделяне на резултатите.
- Използване на резултатите от одитите и мониторинга на системите за ежегодно актуализиране на контролните механизми за качеството и за усъвършенстване на правилата въз основа на реалните резултати и на получената обратна връзка от потребителите.
- Обучение на поне 80% от служителите, работещи с данни, относно очакванията, инструментите и ролите, свързани с качеството на данните веднъж на всеки две години, с цел осигуряване на последователни практики в екипите.

3.5.3 Управление на инциденти

Описание

Управлението на инциденти включва идентифициране, реакция и разрешаване на инциденти, свързани с данните, с цел минимизиране на въздействието върху операциите и гарантиране на интегритета и наличността на данните. Този процес включва установяване на инциденти, провеждане на анализ на първопричините, прилагане на корективни действия и документиране на инцидентите за справка в бъдеще. Ефективното управление на инцидентите гарантира, че данните остават сигурни и надеждни, като по този начин се подкрепя непрекъсваемостта на работния процес и спазването на регулаторните изисквания.

Обхват

- Въвеждане на механизми за мониторинг в реално или почти реално време за критични системи, с цел откриване на аномалии, неоторизиран достъп или нарушения, свързани с данните.



- Прилагане на автоматизирани системи за предупреждение, с цел своевременно уведомяване на определени служители или екипи при установяване на инцидент, свързан с данни.
- Определяне и документиране на стандартизирани протоколи за реагиране при инциденти, включително процедури за ескалация и роли за всеки етап от процеса на реагиране.
- Следва да се гарантира, че са налице механизми за координация между екипите по управление на данни, информационна сигурност, правни и комуникационни въпроси, с цел ефективно овладяване и ограничаване на инцидентите.
- Провеждане на официално разследване след всеки инцидент с данни, за определяне на първопричините, с ясно определени отговорности за анализ и събиране на доказателства.
- Поддържане на структурирана документация за всички инциденти, включително вид, въздействие, предприети действия и срокове за разрешаване.
- Съставяне на вътрешни отчети за всички инциденти със средна до висока значимост, подлежащи на докладване пред съответните органи съгласно приложимите политики и изисквания.
- Ежегоден преглед на процедурите за управление на инциденти, с цел да се гарантира ефективността и да се интегрират анализи от предишни инциденти.
- Актуализиране на вътрешните политики и процедури за екипите въз основа на извлечените поуки, с цел намаляване на повторни инциденти и подобряване на времето за реакция.

3.5.4 Управление на промените

Описание

Управлението на промените включва контролирано и систематизирано управление на измененията в процесите, системите и структурите, свързани с данни. Този процес гарантира, че всички промени се оценяват, одобряват,



документират и прилагат по начин, който минимизира риска от нарушения в операциите и компрометиране на интегритета на данните. Ефективният контрол на промените спомага за поддържането на последователност, качество и съответствие с организационните и регулаторните стандарти.

Обхват

- Установяване на официален, валиден за цялата организация процес за инициране и подаване на заявки за промени, свързани с данни или с процедури по управление на данните.
- Изискване всички подадени заявки за промени да включват ясна документация, очертаваща естеството, целта, обхвата и обосновката на предложената промяна.
- Оценка на всяка предложена промяна по отношение на потенциалното ѝ въздействие върху качеството, интегритета, наличността на данните и оперативната дейност преди одобрение.
- Извършване на оценка на рисковете, ползите и осъществимостта, като част от процеса на преглед на промените, с прилагане на стандартни шаблони за оценка.
- Въвеждане на структуриран, многостепенен процес на одобрение, който включва одобрение от всички заинтересовани страни и от определените органи.
- Координиране на изпълнението с всички екипи, които ще бъдат засегнати, като се осигурява съгласуваност между технически, управленски и оперативни звена.
- Поддържане на централизиран и одитиран регистър на всички одобрени и приложени промени, включително обосновка, анализ на въздействието, срокове и отговорни служители.
- Провеждане на преглед след прилагане на промяната, с цел оценка на резултатите, въздействието и евентуалните непредвидени последици.
- Събиране на поуки и обратна връзка от заинтересованите страни след всеки цикъл на промяна, с цел информирано вземане на решения в бъдеще.



3.5.5 Откриване на данни

Описание

Откриването на данни е процесът, при който се идентифицират, каталогизират и се постига разбиране относно активите от данни в целия публичен сектор. Той включва систематично сканиране и анализ на източници на данни, с цел локализиране, класифициране и документиране на данни чрез стандартизирани метаданни, което ги прави достъпни и използвани за различни цели. Ефективните процеси по откриване на данни дават възможност на организациите да получат по-добра видимост върху наличната информация, да спазват регулаторните изисквания и да вземат информирани решения, основани на яснота относно ресурсите от данни, с които разполагат.

Обхват

- Въвеждане на структуриран процес за идентифициране и документиране на всички активи от данни на организацията, включително метаданни, местоположение, собственост и предназначение.
- Поддържане на централизиран каталог с данни, който включва метаданни, класификации на данните, проследимост на данните и взаимовръзки, който се актуализира редовно и е достъпен за оторизирани потребители.
- Документиране и поддържане на проследимост за критично важни набори от данни, с цел проследяване на произхода, трансформациите и употребата им през целия им жизнен цикъл.
- Записване на метаданни (в съответствие с възприетите, за предпочитане международни, стандарти за метаданни), като формат, честота на актуализиране, изходна система и собственик за всички регистрирани активи от данни.
- Прилагане на процеса по откриване и описване на данни при добавяне на нови системи или набори от данни, така че новите активи да бъдат идентифицирани и каталогизирани още при въвеждането им.



- Редовен преглед и актуализация на каталога с данни (например веднъж на тримесечие), с цел да се отразят промени по структурата или съдържанието на активите от данни.

3.5.6 Процес на формулиране

Описание

Процесът на формулиране е систематичен подход за установяване на ясни, последователни и стандартизирани дефиниции за елементите, термините и понятията, свързани с данните, които се използват в публичната администрация. Този процес гарантира, че всички в организацията споделят общо разбиране относно данните, намалявайки неяснотата и подобрявайки комуникацията и качеството на данните. Процесът на формулиране включва сътрудничество между заинтересованите страни, документиране и текущо управление, с цел да се поддържа последователност в контекста на променящи се бизнес нужди.

Обхват

- Въвеждане на официален процес за дефиниране на елементите и термините, свързани с данни, който включва участието на бизнес звена, отговорници за данни (data stewards), ИТ специалисти и представители на правни или регулаторни звена, когато е приложимо.
- Провеждане на структурирани сесии за дефиниране - като например семинари или интервюта – с цел да се гарантира, че оперативните, техническите и регулаторните перспективи са обхванати и отразени.
- Разработване и одобряване на стандартизирани дефиниции за основни елементи и концепции, свързани с данните, използвани от множество отдели или системи, които са съобразени с националните или международните стандарти.
- Записване на всички одобрени дефиниции в централизирано хранилище с възможност за търсене - в идеалния случай в каталога с данни, с цел да се осигури достъп и възможност за повторна употреба в цялата организация.



- Въвеждане на работен процес за преглед и одобрение на нови или променени дефиниции, с валидиране от експерти в съответната област и одобрение от органите за управление на данните.
- Уведомяване на всички засегнати заинтересовани страни, когато се одобрява, променя или премахва дадена дефиниция чрез официални комуникационни канали или посредством известия в каталога от данни.
- Периодичен преглед на самия процес на дефиниране, с цел да се гарантира, че той продължава да е ефективен, приобщаващ и съобразен с организационните нужди.

3.5.7 Прилагане на политиките

Описание

Елементът, свързан с прилагане на политиките, се отнася до систематичния процес, който гарантира, че политиките, стандартите и процедурите за управление на данните се прилагат и спазват последователно в цялата публична администрация.

Този елемент включва мониторинг на съответствието, идентифициране и отстраняване на отклонения и прилагане на коригиращи действия за поддържане на надеждността, сигурността и качеството на данните. Ефективният контрол по прилагане на политиките гарантира, че практиките за управление на данните са в съответствие с организационните цели и регулаторните изисквания, като по този начин се подпомагат отчетността и прозрачността.

Обхват

- Гарантиране, че 100% от служителите във всички отдели, ангажирани с дейности по управление на данни, имат достъп до най-актуалните политики и потвърждават, че са запознати с тях чрез ориентационно обучение или друг официален механизъм.
- Поддържане на активен мониторинг на критично важни процеси, свързани с данните, с цел проверка на текущото съответствие с политиките за управление на данните, чрез автоматизирани и ръчни проверки.



- Откриване и докладване на инциденти и случаи на несъответствие през утвърдени канали, с документирани процедури за ескалация и реакция.
- Провеждане на редовни вътрешни одити или одити от трети страни (например, ежегодно или веднъж на всеки две години), с цел да се оцени прилагането на политиките за управление на данните и да се идентифицират области за подобрене.
- Координиране на дейностите по контрол на прилагането на политиките в екипите по правни въпроси, човешки ресурси, ИТ и управление на данни, с цел да се гарантира последователен и справедлив подход към нарушенията на политиките.
- Поддържане на записи и документация за извършените действия по контрол на прилагането на политиките, резултатите от одитите и проведените обучения, с цел укрепване на прозрачността и отчетността, вкл. при външен контрол.

3.5.8 Мониторинг

Описание

Мониторингът е процес на непрекъснато проследяване и оценка на дейностите и процесите, както и на спазването на установените политики и стандарти за управление на данните. Този елемент гарантира, че практиките за управление на данните са в съответствие с организационните цели, регулаторните изисквания и стандартите на сектора. Ефективният мониторинг включва използване на автоматизирани инструменти, ръчни прегледи и аналитични механизми за откриване на отклонения, идентифициране на потенциални рискове и осигуряване на надеждността, качеството и сигурността на данните.

Обхват

- Проследяване и преглед на ключови показатели за качеството на данните за всички приоритетни набори от данни.
- Откриване и посочване на отклонения от определените стандарти за данните чрез процеси на мониторинг, с автоматично генериране на предупреждения за критични аномалии.



- Потвърждаване, че основните процеси, свързани с данни (например въвеждане, трансформация и интеграция на данни) се изпълняват в съответствие с документираните процедури и стандартите за управление.
- Осъществяване на мониторинг на моделите за достъп до данни и регистрационните логове/журнали за използването им, с цел да се идентифицира неоторизирана дейност или опити за достъп, като инцидентите се ескалират и се разрешават съгласно протоколите за сигурност.
- Следва да се гарантира, че 100% от критичните системи за данни поддържат активни одитни следи, което позволява проследяване на действията и отчетност при всички потребители и системи.
- Въвеждане на механизъм за обратна връзка, при който резултатите от дейностите по мониторинг се преглеждат веднъж на тримесечие и се използват за усъвършенстване на практиките за управление на данните и на контрола на риска.

3.5.9 Управление на жизнения цикъл на данните

Описание

Управлението на жизнения цикъл на данните описва процесът на управление на данните от създаването и първоначалното им съхранение до архивирането и евентуалното им изтриване. Този елемент се фокусира върху въвеждането на процеси за управление на данните, като гарантира, че данните се управляват последователно и сигурно на всеки етап. Ефективното управление на жизнения цикъл на данните помага на публичните организации да оптимизират използването на данни, да осигурят съответствие, да поддържат качеството на данните и да намалят разходите за съхранение чрез системен контрол върху работата с данните във времето.

Обхват

- Гарантиране, че 100% от новосъздадените или новосъбраните данни отговарят на организационните стандарти за точност, класификация и документиране на метаданни.



- Поддържане на сигурно, достъпно и качествено хранилище за всички активни набори от данни, в съответствие с организационните правила за боравене с данни.
- Редовно прилагане на актуализации, корекции и премахване на дублирани записи, като наборите от данни с висок приоритет се преглеждат поне веднъж на тримесечие.
- Прилагане на правила за достъп и споделяне за всички класифицирани набори от данни, с документирани условия за ползване и разрешения за всяка категория данни.
- Проследяване и регистриране на всички дейности по достъп и използване на данни в критични системи, с цел установяване на неразрешени действия и осигуряване на съответствие.
- Архивиране на всички неактивни, но изисквани по закон набори от данни в сигурни формати, от които данните могат да бъдат възстановени, като процедурите за възстановяване се тестват поне веднъж годишно.
- Привеждане на 100% от архивираните и от активните данни в съответствие с документираните графици за съхранение, които се актуализират веднъж на всеки две години въз основа на законовите и регулаторните рамки.
- Окончателното унищожаване на остарели данни се извършва чрез сигурни и проверими процеси за изтриване или физическо унищожаване, в съответствие с приложимите закони за защита на данните.
- Извършване на годишен преглед на практиките за управление на жизнения цикъл на данните, с цел идентифициране на неефективни практики, рискове или пропуски по отношение на съответствието.

3.5.10 Координация

Описание

Координацията в контекста на управлението на данни се отнася до структурирания процес на съгласуване на усилията, дейностите и комуникацията между различните заинтересовани страни, с цел осигуряване на последователни и



ефективни практики за управление на данните в организацията. Този елемент се фокусира върху хармонизиране на действията на различните екипи, насърчаване на сътрудничеството, разрешаване на конфликтите и оптимизиране на работните процеси за постигане на единни и добре информирани цели в областта на управлението на данните.

Обхват

- Участие на ключови заинтересовани страни от различни звена на публичните организации, включително ИТ, екипи по регулаторно съответствие и управление на данни, във всички основни инициативи за управление на данните, с документиран и редовно актуализирани роли.
- Поддържане на структурирани канали за комуникация (например работни групи или координационни форуми), които са активни поне веднъж годишно, за да съгласуват приоритетите, отговорностите и сроковете за управление на данните.
- Координиране на извършването на промени в процесите с цел минимизиране на припокриванията или прекъсванията между системи и функции, свързани с данни, като се осигуряват плавни преходи.
- Разрешаване на междуведомствени противоречия или несъответствия в прилагането на политиките чрез официален процес на координация или ескалация, с определени срокове за разрешаване, които могат да бъдат проследени.
- Улесняване на съвместното вземане на решения относно споделени активи от данни и въпроси, свързани с управлението, като се гарантира, че оперативните цели не са компрометирани.
- Насърчаване на междуведомственото сътрудничество посредством възлагане на съвместна отговорност за поне една инициатива за управление на данни на година.
- Преглед на ефективността на координационните дейности веднъж годишно въз основа на документиран наблюдения или обратна връзка от участващите екипи с цел установяване на възможности за подобрене.



3.5.11 Управление на доверието

Описание

Управлението на доверието в контекста на управление на данните описва процеса по установяване, поддържане и укрепване на доверието в данните чрез последователни, прозрачни и надеждни практики. То включва мерки, които гарантират точността, сигурността, съответствието и отговорното използване на данните. Управлението на доверието създава доверие у заинтересованите страни, включително крайните ползватели на данни, лицата, отговорни за вземане на решения и външните страни, че данните са надеждни и се управляват в съответствие с установените стандарти и политики.

Обхват

- Осигуряване на прозрачен достъп до метаданните за 100% от публикуваните набори от данни чрез достъпен и добре поддържан каталог с данни.
- Редовни проверки на качеството на наборите от данни с висок приоритет - поне веднъж годишно.
- Поддържане на надеждността на данните чрез валидиране и почистване за всички оперативни набори от данни преди важно използване или публикуване.
- Защита на всички чувствителни данни с въвеждане на контроли за достъп и одитно проследяване, които се преглеждат поне два пъти годишно за неоторизирана дейност или злоупотреба.
- Мониторинг на практиките за боравене с данните в различните отдели, с цел осигуряване на съответствие с регулаторни и етични задължения и политики, като случаите на несъответствие се документират и разрешават.
- Провеждане на самооценка и на външни одити на управлението на данните поне веднъж годишно за области с висок риск, с проследяване на действията за отстраняване на установените слабости.
- Осигуряване на открита комуникация с вътрешни и външни заинтересовани страни относно начина, по който данните се използват и



управляват, чрез редовни срещи за актуализация, брифинги или табла с данни.

- Събиране на обратна връзка от крайни ползватели на данни и от заинтересованите страни поне два пъти годишно, с цел да се идентифицират проблеми, свързани с доверието и да се предприемат коригиращи действия, когато е необходимо.
- Разглеждане на всички потвърдени инциденти или пробиви в сигурността в рамките на определените срокове, като резюмета на предприетите действия се споделят със засегнатите страни с цел запазване на прозрачността и доверието.

4. КАТЕГОРИЯ ТЕХНОЛОГИИ

4.1. Описание

Категорията ТЕХНОЛОГИИ е насочена към използването на инструменти и системи в подкрепа на дейностите по управление на данните. Тя включва управление на метаданни, инструменти за качество на данните, решения за разпореждане с данни и стабилна системна архитектура, за да се гарантира, че данните се управляват по правилен начин, защитени са и са използвани ефективно. Тази категория осигурява технологичната основа, необходима за осъществяването на управлението на данни и за улесняване на безпроблемни операции с данни в целия публичен сектор. Тя играе ключова роля за осигуряване на ефективни процеси за данни и спазване на предварително определени и договорени стандарти.

4.2. Цел

Целта на категорията ТЕХНОЛОГИИ е да осигури необходимата технологична инфраструктура в подкрепа на ефективното управление на данните в публичните институции. Тя предвижда предоставянето и, при възможност, интегрирането на различни инструменти и системи за данни – като управление на метаданни, проследяване на данните и инструменти за управление на качеството в



единна рамка, която подобрява събирането, съхранението, преноса, управлението и използването на данни в публичния сектор.

4.3. Рискове

Технологичната основа е от решаващо значение за управлението на данните, но редица рискове следва да бъдат отчетени, за да се гарантират сигурността, съвместимостта и безпроблемното прилагане. Непълното управление на метаданните поради технологични проблеми или липси може да доведе до погрешно тълкуване на данните, оперативна неефективност и цялостни пропуски в управлението, особено що се отнася до инструментите за управление на метаданни и инструментите за управление на разпореждане с данни. По подобен начин, пропуски в качеството на данните, породени от слабости при валидирането или интегрирането на инструментите за управление на качеството, могат да станат причина за скрити грешки, които подкопават надеждността на информацията и процесите по вземане на решения.

Нарушенията в сигурността на данните са друг критичен риск, тъй като недостатъчните механизми за контрол на достъпа и сигурността могат да изложат чувствителни данни на неоторизиран достъп. Освен това, липсата на интегрирана архитектура и свързаност между системи за основни или референтни данни може да доведе до изолирани масиви от данни, което ограничава достъпността и използваемостта на информацията, затруднява управлението и води до дублиране на дейности. Ниско ниво на използване на технологиите за управление на данни от потребителите – поради прекалена сложност или недостатъчна поддръжка – може да обезсмисли други вече прилагани инструменти, като решения за проследимост и разпореждане с данни, и да ограничи ефективността им.

Други рискове включват предизвикателства, свързани с мащабируемостта, при които технологиите не успяват да поддържат нарастващите обеми и сложност на данните, което ограничава дългосрочната устойчивост на системната архитектура и инструментите за качество на данните. Неспазване на регулаторни изисквания, породено от разминавания между функционалността на системите и законовите норми – с потенциални правни и финансови последици. Освен това,



забавянията в разрешаването на проблеми – в резултат на неефективно управление на технологиите за контрол на достъпа – могат да нарушат критични процеси на управление. Проблеми с интегритета на данните, причинени от прекомерна автоматизация без необходима проверка и валидация – с негативен ефект върху точността и надеждността на данните. Управлението на тези рискове изисква поетапно прилагане, внимателно разширяване, стратегически технологични инвестиции, силен надзор и ангажираност от страна на потребителите.

4.4. Изисквания за съответствие

- Използване на надеждни системи за управление на достъпа, с цел защита на чувствителните данни и метаданни от неоторизиран достъп.
- Извършване на редовни одити на технологичните процеси и инструменти, с цел да се гарантира съответствие с регулаторните изисквания и организационните политики.
- Поддържане на подробни записи на дейности, свързани с технологиите, включително системни промени и практики за управление на данните.
- Прилагане на криптиране и сигурни методи за съхранение на чувствителни данни, като се гарантира спазването на най-добрите практики и законовите изисквания.
- Осигуряване на програми за обучение на потребителите, с цел да се гарантира ефективното използване и разбиране на технологиите за управление на данни.
- Въвеждане на технологии, които могат да се мащабират и да се адаптират към променящите се нужди на управлението на данни и регулаторните промени.
- Гарантиране, че инструментите за качество на данните отговарят на организационните стандарти за точност, пълнота и навременност.
- Разработване и поддържане на ясни протоколи за реакция при инциденти, свързани със сигурността и съответствието с технологиите за данни.



- Редовно актуализиране и усъвършенстване на технологичните инструменти и практики, в синхрон с напредъка в областта на управлението на данни и регулаторните изисквания.

4.5. Елементи на категорията ТЕХНОЛОГИИ



Фигура 5. Елементи на категорията ТЕХНОЛОГИИ

4.5.1 Инструменти за управление на метаданни (Каталог от данни)

Описание

Инструментите за управление на метаданни, често наричани каталози от данни, са технологии, предназначени за създаване, управление и използване на метаданни с цел организиране и разбиране на информационните масиви в рамките на организацията. Тези инструменти позволяват каталогизиране и класифициране на данните и предоставят информация относно произхода, контекста и начините на използване на данните. Добре разработеният каталог подпомага откриването на данните, управлението им и постигането на съответствие, като осигурява централизиран достъп до метаданни и повишава прозрачността, качеството и приложимостта на данните.

Обхват

- Гарантиране, че 100% от критичните активи от данни са регистрирани в хранилище за метаданни, като са записани основните им атрибути, включително източник, формат, собственост и честота на актуализация.
- Осигуряване на видимост в организацията по отношение на проследимостта на данните във всички основни системи, позволявайки



на ползвателите да обследват произхода и трансформациите на данните през целия им жизнен цикъл.

- Даване на възможност на потребителите да класифицират всички регистрирани активи от данни чрез стандартизирани етикети, категории и дефиниции, с цел подобряване на възможностите за откриване и използване на данните.
- Осигуряване на съответствие на метаданните с организационните модели на управление чрез използване на одобрени таксономии и онтологии, които се прилагат по унифициран начин във всички звена.
- Улесняване на анализа на въздействието, базиран на метаданни, като се дава възможност на заинтересованите страни да установят зависимостите при промени в източниците на данни или в системите.
- Поддържане на механизми за контрол и одобрение на версиите на метаданните, което да гарантира, че промените на дефинициите или класификациите са управлявани, проследими и преглеждани.
- Насърчаване на сътрудничество чрез предоставяне на споделена платформа, в която отговорниците за данни и анализаторите могат да добавят пояснения (анотации), да обогатяват и валидират метаданни в реално време.

4.5.2 Инструменти за управление на процесите, свързани с данни

Описание

Инструментите за управление на процесите, свързани с данни (data stewardship tools) подпомагат управлението и контрола върху данните от гледна точка на изпълнението на ролите и отговорностите на отговорниците за данни (data stewards). Инструментите за управление на данни дават възможност на отговорниците за данни (data stewards) да прилагат стандарти за данни, да управляват работните потоци на данните и да проследяват състоянието на проблеми, свързани с данните, като в крайна сметка подобряват интегритета, точността и надеждността на данните в организацията.



Обхват

- Осигуряване на възможност за мониторинг на качеството на данните от отговорниците (data stewards) чрез ключови показатели и тенденции, с редовен преглед на всички приоритетни масиви.
- Гарантиране, че всички проблеми с качеството на данните и съответствието се регистрират, приоритизират и проследяват чрез система за управление на инциденти, като статусът им е видим за съответните заинтересовани страни.
- Даване на възможност на отговорниците за данни (data stewards) да определят и прилагат одобрени политики за управление, стандарти за данни и бизнес правила за регистрираните набори от данни, като за всички актуализации се поддържа история на промените.
- Поддържане на активни работни процеси за управление на данните за основните процеси, като преглед, одобрение и валидиране на данни, което осигурява навременно изпълнение и документиран резултат.
- Поддържане на базиран на роли достъп до задачите по управление на данни, така че отговорностите да са ясно разпределени и съгласувани със структурата на собственост върху данните.
- Улесняване на координацията между функции чрез предоставяне на възможности за комуникация между отговорници, собственици и бизнес потребители – включително добавяне на коментари, споделяне на документи и обсъждания в самата платформа.
- Поддържане на логове от одитите за всички дейности по управление на данни, включително оценки на качеството, решения на проблеми и действия за контрол на прилагането на правила, с възможност за вътрешен и външен преглед.

4.5.3 Проследяване на данните

Описание

Този елемент се отнася до технологиите, които проследяват и визуализират движението на данните – от техния произход, през различни трансформации,



системи и процеси, до крайната им точка на използване. Тези инструменти дават възможност на организациите да разберат как се променят и използват данните във времето, като осигуряват прозрачност по отношение на зависимости, трансформации и употреба на данните. Те са от съществено значение за гарантиране на прозрачност, качество и съответствие, като осигуряват ясна представа за създаването, модифицирането и използването на данните в рамките на организацията.

Обхват

- Описване на пътя на данните през системи, приложения и процеси, от източника им до тяхното крайно потребление.
- Визуализиране на трансформациите, движенията и зависимостите на данните в ясен и интерактивен формат, който подпомага разбирането на сложни потоци от данни.
- Осигуряване на възможност за оценка на въздействието от промени в източниците, трансформациите или процесите върху свързаните данни и генерираните отчети.
- Предоставяне на информация относно логиката на трансформациите, скриптовете и параметрите, с цел осигуряване на прозрачност и възпроизводимост.
- Интеграция с инструменти за управление на метаданни с цел обогатяване на проследимостта с контекстуална информация – като собственост, дефиниции и класификации на данните.
- Поддържане на подробни записи относно проследяването на данните, с цел да се подпомогне спазването на политиките за управление на данните и на регулаторните изисквания.
- Предоставяне на подробна документация относно проследяването на данните и одитни следи за демонстриране на съответствие с правилата за работа с данни и стандарти за трансформация.



4.5.4 Достъп и сигурност

Описание

Технологиите за контрол на достъпа и сигурността са критично важни за защитата на информационните активи, като гарантират, че само упълномощени лица могат да имат достъп, да извършват промени или да управляват данни съгласно предварително определени политики и стандарти. Тези технологии включват инструменти за управление на идентичността и достъпа, криптиране, удостоверяване и мониторинг.

Обхват

- Въвеждане на системи за управление на потребителските идентичности и контрол на достъпа до данни и системи въз основа на роли и права на достъп.
- Въвеждане на многофакторна автентикация (MFA) и единна система за вход/вписване (SSO), с цел да се подобри сигурността и да се улесни достъпа на потребителите.
- Използване на технологии за криптиране за защита на данните, както при съхранение, така и при пренос, като се гарантира, че чувствителната информация остава нечетима за неоторизирани потребители.
- Дефиниране и прилагане на подробни политики за контрол на достъпа, които уточняват кой може да чете, редактира или изтрива данни според потребителските роли и нивото на чувствителност на информацията.
- Внедряване на инструменти за мониторинг и регистриране на потребителската активност (логване), включително достъпване, модификации и изтриване на данните.
- Прилагане на техники за маскиране и анонимизиране на данни, с цел защита на чувствителни данни извън продукционните среди или при споделяне с външни страни.
- Гарантиране на запазването на поверителността и неприкосновеността на данните, без това да нарушава тяхната използваемост.



4.5.5 Инструменти за управление на качеството на данните

Описание

Инструментите за управление на качеството на данните са технологични решения, създадени с цел оценка, мониторинг и подобряване на качеството на данните в рамките на организацията. Те предоставят функционалности за профилиране и валидиране на данни, което позволява на организациите да поддържат високи стандарти за точност, пълнота, последователност и надеждност на данните.

Обхват

- Поддържане на автоматизирана оценка на ключови измерения на качеството на данните чрез използването на предварително дефинирани показатели за 100% от приоритетните набори от данни, като резултатите следва да са достъпни за екипите, които са ангажирани с управлението.
- Осигуряване на възможности за въвеждането на предварително дефинирани правила за валидиране на данни и бизнес правила, за да се гарантира съответствие с вътрешните стандарти и външните регулаторни изисквания.
- Автоматично откриване и маркиране на често срещани проблеми с качеството на данните (например дублирани данни, несъответствия във форматите и невалидни записи), като се прилагат или планират корективни действия.
- Обогаляване на наборите от данни чрез добавяне на валидирана информация от вътрешни системи или от оторизирани външни източници, което подобрява пълнотата и използваемостта на данните.
- Генериране на сигнали и известия при критични проблеми с качеството на данните, за да се осигури навременна проверка и разрешаване на проблемите от отговорните екипи.
- Регистриране на всички дейности, свързани с качеството на данните, включително идентифициране на проблеми, стъпки за разрешаването им и одобрения, в журнали, които могат да бъдат одитирани и които са поддържани от платформи за управление.



- При възможност, интегриране с инструменти за метаданни, за проследяване на произхода на данните и за управление на процесите, свързани с данни, с цел да се осигури унифицирана информация относно състоянието, произхода и отчетността на данните.
- Въвеждане на автоматизирани работни процеси за проследяване и ескалиране на проблеми с качеството на данните, чрез възлагане на задачи на съответните отговорници (stewards) или собственици на данни (data owners) за извършване на последващи действия и разрешаване на проблемите.

4.5.6 Основни/референтни данни

Описание

Инструментите за управление на основни и референтни данни (MDM/RDM) са технологии, предназначени да поддържат единен, последователен и точен модел на ключови обекти, като граждани, услуги, доставчици и местоположения. Тези инструменти подпомагат централизирането, стандартизирането и синхронизирането на основните и референтните данни в различните системи, така че всички бизнес процеси и приложения да работят с една и съща основна информация.

Обхват

- Поддържане на централизирано хранилище за основни и референтни данни, като се гарантира, че поне 90% от критичните обекти (например лица, организации, места) са последователно представени в основните системи (базовите регистри).
- Прилагане на стандарти и оперативни правила за именуване, класифициране и форматиране на основни/референтни данни, с цел гарантиране на унифицираност.
- Определяне на ясна собственост върху данните за всички основни/референтни домейни, с документиран работен процес за създаване, валидиране и одобрение на данни.



- Синхронизиране на актуализациите на основните и референтните данни в свързани системи в определени времеви рамки (например, в почти реално време или ежедневно синхронизиране), като по този начин се осигурява съгласуваност и се ограничава дублирането.
- Управление на пълния жизнен цикъл на основните/референтни данни, от първоначалното им въвеждане през различните версии, актуализации и изтеглянето им от употреба, с подходящи механизми за контрол и одитни следи.
- Архивиране на остарели или отпаднали основни/референтни данни съгласно политиките за съхранение, като по този начин се осигурява релевантността и ефективността на централното хранилище.

4.5.7 Системна архитектура

Описание

Системната архитектура, от гледна точка на управлението на данни, се отнася до проектирането и организацията на системите за данни, платформите и технологиите, които поддържат ефективното управление на данните в дадена организация. Тя обхваща документирането на екосистемата от данни, интеграцията, комуникацията и сигурността на системите за данни, с цел да се гарантира ефективното движение, достъпността и управлението на активите от данни.

Обхват

- Осигуряване на оперативна съвместимост на всички основни системи за данни чрез интегрирана архитектура, която позволява безпрепятствен обмен на данни както в локална, така и в облачна среда.
- Поддържане на последователен достъп и поток на данни чрез свързване на поне 90% от критично важните системи чрез стандартизирани интеграционни и междинни слоеве.
- Поддържане на нарастващите обеми данни и развиващите се бизнес нужди с помощта на мащабируема архитектура, която поддържа



ефективността и надеждността на управлението на данни при разширяване на системата.

- Експлоатация на централизирани или федерирани решения за съхранение на данни (например, хранилища за данни, езера от данни и др.), които позволяват ефективно извличане, анализ и управление на жизнения цикъл на данните.
- Осигуряване на капацитет/функционалност за управление на метаданни, контрол по качеството на данните и проследяване на данните в архитектурата, като се гарантира, че тези функции са технологично обезпечени по дизайн.
- Автоматизиран мониторинг на съответствието чрез интегриране на платформи за управление на данни, в системната архитектура.
- Въвеждане и редовно тестване на системи за възстановяване след срыв и за резервни копия/архивиране на данни, с цел да се гарантира възстановяването на данните в рамките на определените срокове за всички критични активи.