ПОЛИТИКА ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ПОЛИТИКА
ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ
МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Въведение

Настоящата политика е разработена въз основа на насоките в Общия регламент за защита на личните данни, съгласно който защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки (ТОМ), за да се гарантира изпълнението на изискванията на Общия регламент за защита на личните данни.

Раздел I.

Основни принципи

1. За всяка конкретна обработка институцията осигурява подходящи технически и организационни мерки за защита на личните данни, отчитайки:

- Достиженията на техническия прогрес.
- Разходите за прилагане на мерките.
- Естеството на обработването.
- Обхвата на обработването.
- Контекста и целите на обработването.
- Възможните рискове за правата и свободите на физическите лица.
- Рискове от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

2. Основен принцип, който институцията спазва, е да не се обработват повече от необходимите лични данни, като това се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

3. Данните следва да се обработват само от лицата, обработващи тези данни по указание на администратора.

4. Процесът по обработката следва да бъде документиран.

Раздел II.

Насоки за изграждане на система от технически и организационни мерки (ТОМ) за защита на личните данни

5. С оглед на важното значение на ТОМ по отношение на налаганите глоби от надзорния орган, институцията следва да реализира мерки, които се основават на:

- обучение на служителите, обработващи лични данни;
- документална обезпеченост на процесите, включително документиране на самите процеси;
- мониторинг на обработването на данни за своевременно откриване на пробиви в сигурността;
- залагане на изискванията на ОРЗД в нормалните дейности на институцията (избор на доставчици, използване на информационни системи и т.н.).

Раздел III.

Приложимо ниво на риск

6. С оглед на множеството паралелни дейности, които се извършват в институцията, тя възприема единна оценка на риска на всички свои дейности, прилагайки най-високия, установен такъв.

7. До наличието на официална национална методология за определяне нивото на риска, институцията приема, че нивото на риск на обработването на данни като администратор се приема за „ниско“ – неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

8. В случай, че институцията е обработващ данни, съответните технически и организационни мерки се определят в договора със съответния администратор или нормативен акт, който регулира това отношение. Институцията си запазва правото самостоятелно да въведе допълнителни мерки за сигурност, които смята за необходими.

Раздел IV.

Технически и организационни мерки за защита на личните данни

9. Мерките, посочени по-долу, се основават на възприетото ниво на риск в т.7.

10. Не всички мерки е възможно да се отнасят към обичайната дейност на институцията, но е възможно необходимостта от тях да възникне при дейността на обработващите за институцията данни от трети страни или такива, които създават специфични решения за нея.

11. Техническите и организационни мерки се прилагат, доколкото се поддържа от функционалността на съответното устройство или операционна система, и се използват от институцията във връзка с осъществяването на съответния процес.

12. Мерки, насочени към документалното и оперативното изпълнение на мерките за защита на личните данни:

- Налична е политика за защита на личните данни;
- Налична е процедура за действие при нарушение на личните данни;
- Описание на техническите и организационните мерки по отношение на защита на лични данни.
- Субсидиарно се прилагат и:
  - Политика за информационна сигурност;
  - План за непрекъсваемост на работните процеси.

13. Мерки, насочени към служителите:

- Информиране и засилване на чувствителността на служителите по отношение на обработването на лични данни, включително чрез провеждането на начални обучения;
- Налагане на задължителна инструкция за допустимата употреба на компютърни устройства на институцията включително налагане на дисциплинарни наказания при нейното нарушаване;
- Служителите биват информирани и подписват декларация за поверителност.

14. Мерки, насочени към достъпване на информационните системи на институцията.

- Всеки потребител има свой уникален акаунт, който следва да не споделя с никой друг;
- Налице е политика за сложност на паролите за достъп до акаунта, обхващаща всички устройства на институцията (вкл. смартфони, таблети, лаптопи, стационарни компютри, сървъри и т.н.);
- Потребителите следва да променят редовно своята парола, по възможност наложено от самите електронни системи;
- Неуспешните опити за достъп до акаунтите следва да бъде ограничен;

15. Мерки насочени към управление на даването на достъпи до информационните системи на институцията.

- Потребителите имат различни акаунти (профили) за отделните задачи, които извършват;
- Всички ненужни права (например вследствие на напускане или преместване) следва да се премахват своевременно;
- Всички стари права подлежат на редовен преглед и премахване при необходимост поне веднъж в годината;

16. Мерки насочени към проследяване на достъпа и управление на инциденти.

- Система за създаване и поддържане на логове на достъпа до ресурсите с лични данни;
- Потребителите следва да бъдат информирани за поддържаните логове;
- Логовете не могат да бъдат достъпвани или променяни от неоторизиран персонал;
- Наличие на процедури за нотификация при пробив в сигурността на личните данни.

17. Мерки насочени към сигурността на работните станции.

- Използване само на лицензиран софтуер;
- Регулярно обновяване на антивирусните софтуери;
- Инсталирана софтуерна стена;
- Забрана за инсталиране на неоторизиран софтуер;
- Ограничаване използването на преносима памет;
- Процедури за автоматично заключване на сесиите;
- Редовно инсталиране на критични обновявания;
- 7.8. Ограничаване използването на Интернет, а ако е невъзможно - използване на софтуери за филтриране на уеб страници и определени действия;
- Използване на стандартните опции за криптиране на дисковете за съхранение на информация на операционните системи;
- Взимане на съгласие преди интервенция от страна на администратора върху работната машина на потребителя.

18. Мерки насочени към сигурността на използваните мобилни устройства.

- Криптиране на мобилните устройства;
- Възможност за отдалечено проследяване на откраднато/загубено устройство;
- Регулярно създаване на резервни копия и синхронизация на данните;
- Смартфоните изискват отключване посредством определено действие, свързано със сигурността.

19. Мерки, насочени към сигурността на вътрешната компютърна мрежа.

- Ограничаване мрежовите потоци само до най-необходимото;
- Осигуряване на достъп на мобилните изчислителни устройства посредством VPN;
- Отделяне на Wi-Fi мрежата от другите мрежи;
- Прилагане на WPA2 или WPA2-PSK за Wi-Fi мрежите;
- Провеждане на ежегодни тестове за проникване (външни).

20. Мерки, насочени към сигурността на сървърите.

- Ограничаване на достъпа до административни инструменти само за оторизирани лица;
- Незабавна инсталация на критични обновявания;
- Осигуряване на наличността на данните;
- Мерки насочени към сигурността на уеб страниците/уеб системи на институцията Използване на TLS протокол;
- Парола или потребителско име не се предават в URL;
- Категорийни данни, които могат да разкрият лични данни, не се предават в URL;
- Основните данни, които могат да послужат за разпознаване, са криптирани;
- Поставяне на банер за съгласие за бисквитките, които не са необходими за предоставяне на основните услуги.

21. Мерки, насочени към осигуряване на непрекъсваемостта на организационните процеси.

- Създаване на регулярни резервни копия;
- Съхранение на резервните копия на сигурно място;
- Планират се мерки за сигурност за предаване на резервните копия;
- Планиране и тестване на непрекъсваемостта на организационните процеси.

22. Мерки, насочени към осигуряване на сигурността на архивирането.

- Прилагане на специфични процедури за достъп до архивираните данни;
- Унищожаване на старите архиви по сигурен начин.

23. Мерки, насочени към осигуряване на мониторинг върху унищожаването на носители на данни.

- Записване на възможните интервенции в регистър;
- Наблюдаване на интервенциите на трети страни от официално лице на институцията;
- Изтриване на данните от носителя преди неговото унищожаване.

24. Мерки, насочени към контрол на доставчиците.

- Специални клаузи в договорите с доставчиците;
- Предвидени условия за връщане или унищожаване на данните;
- Контрол върху ефективността на предоставените гаранции (одити по сигурността, визити и т.н.).

25. Мерки, насочени към сигурността на обмен на данни с трети страни.

- Криптиране на данните преди тяхното изпращане;
- Предаване на секрета разделно и посредством различен канал;
- Изрична проверка, че е подаден верният получател;
- Прикачване на съобщение за конфиденциалност към всяко изпратено съобщение;
- Използване само на служебни електронни пощи, когато съобщението се изпраща по имейл.

26. Мерки, насочени към физическата защита на помещенията

- Ограничаване на достъпа до помещенията посредством заключени врати;
- Инсталиране на аларма против взлом и периодичната им проверка;
- Използване на заключващи шкафове или каси за съхраняване на личните данни и/или преносимите изчислителни устройства;
- Следване на политика на „чисто бюро“.

27. Мерки, насочени към разработчици на електронни системи за институцията.

- Тестването на електронни системи се извършва само с фиктивни или анонимизирани данни;
- В случай на наличието на опционалности, насочени към поверителността на информацията, предлагане на настройки за тях на крайния потребител.

28. Мерки, в случай на необходимост от използване на криптографски услуги.

- Използване на признати алгоритми, софтуери и библиотеки;
- Запазване защитени секрета и криптографските ключове.

Раздел V.

Трети страни, обработващи данни

29. В случай на използване на трети страни като обработващи данни, институцията използва само такива обработващи, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки за защита на личните данни. Тези мерки следва да бъдат сходни по обхват на тези, които са определени в раздел „Технически и организационни мерки за защита на личните данни“ от тази политика. Обработването се възлага чрез договор, в който изрично са посочени поне:

- Предмет на обработването;
- Срок на обработването;
- Естеството и целта на обработването;
- Вида лични данни;
- Категориите субекти на данни;
- Задълженията и правата на администратора;
- Необходимостта от писмено разрешение от страна на институцията за използване на други обработващи от обработващия данни;
- Обработващият действа само по указания на администратора;
- Обработващият гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
- Обработващият подпомага администратора с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни.

Раздел VI.

Обновяване на техническите и организационните мерки (ТОМ)

30. За целта на поддържане на ТОМ в актуално състояние с оглед на условията посочени в т.1.1-1.7, всяка година СЗД/ДЛЗД извършва преглед и при необходимост координира необходимостта от промени със засегнатите звена в институцията.