

## **ПОЛИТИКА ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА**

### **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:
  - 1.1. Достиженията на техническия прогрес.
  - 1.2. Разходите за прилагане на мерките.
  - 1.3. Естеството на обработването.
  - 1.4. Обхвата на обработването.
  - 1.5. Контекста и целите на обработването.
  - 1.6. Възможните рискове за правата и свободите на физическите лица.
  - 1.7. 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:
  - 5.1. обучение на служителите, обработващи лични данни;
  - 5.2. документална обезпеченост на процесите, включително документиране на самите процеси;
  - 5.3. мониторинг на обработването на данни за своевременно откриване на пробиви в сигурността;
  - 5.4. 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**

Политика за техническите и организационни мерки за защита на личните данни

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:
  - 12.1. Налична е политика за защита на личните данни;
  - 12.2. Налична е процедура за действие при нарушение на личните данни;
  - 12.3. Описание на техническите и организационните мерки по отношение на защита на лични данни.
  - 12.4. Субсидиарно се прилагат и:
    - 12.4.1. Политика за информационна сигурност;
    - 12.4.2. План за непрекъсваемост на работните процеси.
13. Мерки, насочени към служителите:
  - 13.1. Информирание и засилване на чувствителността на служителите по отношение на обработването на лични данни, включително чрез провеждането на начални обучения;
  - 13.2. Налагане на задължителна инструкция за допустимата употреба на компютърни устройства на институцията включително налагане на дисциплинарни наказания при нейното нарушаване;
  - 13.3. Служителите биват информирани и подписват декларация за поверителност.
14. Мерки, насочени към достъпване на информационните системи на институцията.
  - 14.1. Всеки потребител има свой уникален акаунт, който следва да не споделя с никой друг;
  - 14.2. Налице е политика за сложност на паролите за достъп до акаунта, обхващаща всички устройства на институцията (вкл. смартфони, планшети, лаптопи, стационарни компютри, сървъри и т.н.);

Политика за техническите и организационни мерки за защита на личните данни

- 14.3. Потребителите следва да променят редовно своята парола, по възможност наложено от самите електронни системи;
- 14.4. Неуспешните опити за достъп до акаунтите следва да бъде ограничен;
15. Мерки насочени към управление на даването на достъпи до информационните системи на институцията.
  - 15.1. Потребителите имат различни акаунти (профили) за отделните задачи, които извършват;
  - 15.2. Всички ненужни права (например вследствие на напускане или преместване) следва да се премахват своевременно;
  - 15.3. 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.
  - 16.1. Система за създаване и поддържане на логове на достъпа до ресурсите с лични данни;
  - 16.2. Потребителите следва да бъдат информирани за поддържаните логове;
  - 16.3. Логовете не могат да бъдат достъпвани или променяни от неоторизиран персонал;
  - 16.4. Наличие на процедури за нотификация при пробив в сигурността на личните данни.
17. Мерки насочени към сигурността на работните станции.
  - 17.1. Използване само на лицензиран софтуер;
  - 17.2. Регулярно обновяване на антивирусните софтуери;
  - 17.3. Инсталирана софтуерна стена;
  - 17.4. Забрана за инсталиране на неоторизиран софтуер;
  - 17.5. Ограничаване използването на преносима памет;
  - 17.6. Процедури за автоматично заключване на сесиите;
  - 17.7. Редовно инсталиране на критични обновявания;
  - 17.8. Ограничаване използването на Интернет, а ако е невъзможно - използване на софтуери за филтриране на уеб страници и определени действия;
  - 17.9. Използване на стандартните опции за криптиране на дисковете за съхранение на информация на операционните системи;
  - 17.10. Взимане на съгласие преди интервенция от страна на администратора върху работната машина на потребителя.
18. Мерки насочени към сигурността на използваните мобилни устройства.
  - 18.1. Криптиране на мобилните устройства;
  - 18.2. Възможност за отдалечено проследяване на откраднато/загубено устройство;
  - 18.3. Регулярно създаване на резервни копия и синхронизация на данните;
  - 18.4. Смартфоните изискват отключване посредством определено действие, свързано със сигурността.
19. Мерки, насочени към сигурността на вътрешната компютърна мрежа.
  - 19.1. Ограничаване мрежовите потоци само до най-необходимото;
  - 19.2. Осигуряване на достъп на мобилните изчислителни устройства посредством VPN;
  - 19.3. Отделяне на Wi-Fi мрежата от другите мрежи;
  - 19.4. Прилагане на WPA2 или WPA2-PSK за Wi-Fi мрежите;
  - 19.5. Провеждане на ежегодни тестове за проникване (външни).

Политика за техническите и организационни мерки за защита на личните данни

20. Мерки, насочени към сигурността на сървърите.
  - 20.1. Ограничаване на достъпа до административни инструменти само за оторизирани лица;
  - 20.2. Незабавна инсталация на критични обновявания;
  - 20.3. Осигуряване на наличността на данните;
  - 20.4. Мерки насочени към сигурността на уеб страниците/уеб системи на институцията Използване на TLS протокол;
  - 20.5. Парола или потребителско име не се предават в URL;
  - 20.6. Категорийни данни, които могат да разкрият лични данни, не се предават в URL;
  - 20.7. Основните данни, които могат да послужат за разпознаване, са криптирани;
  - 20.8. 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.
  - 21.1. Създаване на регулярни резервни копия;
  - 21.2. Съхранение на резервните копия на сигурно място;
  - 21.3. Планират се мерки за сигурност за предаване на резервните копия;
  - 21.4. Планиране и тестване на непрекъсваемостта на организационните процеси.
22. Мерки, насочени към осигуряване на сигурността на архивирането.
  - 22.1. Прилагане на специфични процедури за достъп до архивираните данни;
  - 22.2. Унищожаване на старите архиви по сигурен начин.
23. Мерки, насочени към осигуряване на мониторинг върху унищожаването на носители на данни.
  - 23.1. Записване на възможните интервенции в регистър;
  - 23.2. Наблюдаване на интервенциите на трети страни от официално лице на институцията;
  - 23.3. Изтриване на данните от носителя преди неговото унищожаване.
24. Мерки, насочени към контрол на доставчиците.
  - 24.1. Специални клаузи в договорите с доставчиците;
  - 24.2. Предвидени условия за връщане или унищожаване на данните;
  - 24.3. 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.
  - 25.1. Криптиране на данните преди тяхното изпращане;
  - 25.2. Предаване на секрета разделно и посредством различен канал;
  - 25.3. Изрична проверка, че е подаден верният получател;
  - 25.4. Прикачване на съобщение за конфиденциалност към всяко изпратено съобщение;
  - 25.5. Използване само на служебни електронни пощи, когато съобщението се изпраща по имейл.
26. Мерки, насочени към физическата защита на помещенията
  - 26.1. Ограничаване на достъпа до помещенията посредством заключени врати;
  - 26.2. Инсталиране на аларма против взлом и периодичната им проверка;
  - 26.3. Използване на заключващи шкафове или каси за съхраняване на личните данни и/или преносимите изчислителни устройства;
  - 26.4. Следване на политика на „чисто бюро“.

Политика за техническите и организационни мерки за защита на личните данни

27. Мерки, насочени към разработчици на електронни системи за институцията.
  - 27.1. Тестването на електронни системи се извършва само с фиктивни или анонимизирани данни;
  - 27.2. 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.
  - 28.1. Използване на признати алгоритми, софтуери и библиотеки;
  - 28.2. 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:
  - 29.1. Предмет на обработването;
  - 29.2. Срок на обработването;
  - 29.3. Естеството и целта на обработването;
  - 29.4. Вида лични данни;
  - 29.5. Категориите субекти на данни;
  - 29.6. Задълженията и правата на администратора;
  - 29.7. Необходимостта от писмено разрешение от страна на институцията за използване на други обработващи от обработващия данни;
  - 29.8. Обработващият действа само по указания на администратора;
  - 29.9. Обработващият гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
  - 29.10. 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.

Директор: .....

*/инж.Галина Калмушка/*