Вътрешна политика, правила и процедури за обработване на лични данни при използване и наемане на облачни услуги

(приети с Решение № 1579 на Висшия адвокатски съвет от 06.02.2025 г.)

СЪДЪРЖАНИЕ

Въведение

Настоящата политика определя принципите, правилата и процедурите, които Висшият адвокатски съвет („ВАдвС“/ „Организацията“) прилага за обработка на лични данни на физически лица при използване и наемане на облачни услуги. Политиката е създадена в съответствие с Регламент (ЕС) 2016/679 (Общ регламент за защита на данните - ОРЗД), местното законодателство и най-добрите практики в областта на информационната сигурност.

Настоящата политика е приета и във връзка с Разпореждане на Комисията за защита на личните данни („КЗЛД“) съгласно Решение № ППН-01-58 от 05.12.2024 г., като същата следва да бъде периодично актуализирана, както е описана по-долу с оглед развитието на технологиите и приложимото законодателство.

Цели

Член 1: Цели на политиката

1.1. Осигуряване на законосъобразно, добросъвестно и прозрачно обработване на личните данни.

1.2. Гарантиране на наличност, цялостност и поверителност на личните данни чрез подходящи технически и организационни мерки.

1.3. Създаване на ясни правила за обработката на лични данни при използване и наемане на облачни услуги.

1.4. Утвърждаване на доверие сред субектите на данни, чиито данни са под контрола на ВАдвС чрез спазване на адекватни стандарти за защита на данните с оглед текущото технологично развитие.

1.5. Осигуряване на ефективна отчетност и възможност за доказване на съответствие с изискванията на ОРЗД.

Обхват

Член 2: Приложно поле на политиката

2.1. Настоящата политика се прилага за всички дейности, свързани с обработката на лични данни при използване и наемане на облачни услуги от Организацията.

2.2. Политиката обхваща всички служители, партньори, доставчици и трети лица, които участват в обработката на лични данни от името на Организацията.

2.3. Политиката включва всички видове лични данни, обработвани чрез облачни платформи, независимо от тяхното местоположение (в рамките на ЕС или извън него).

2.4. ВАдвС използва доставчици на облачни услуги, чиито центрове за данни се намират единствено на територията на ЕС и ЕИП или в държави, за които Европейската комисия е приела с надлежно решение относно адекватното ниво на защита за безопасни и надеждни потоци от данни. По изключение могат да бъдат използвани доставчици на облачни услуги, чиито центрове за данни са извън териториите по предходното изречение, но единствено след положително становище от длъжностното лице по защита на данните и при спазване на правилата, предвидени за такива трансфери, в ОРЗД.

Дефиниции

Член 3: Основни термини

3.1 Лични данни: Всяка информация, свързана с идентифицирано или идентифицируемо физическо лице.

3.2. Обработващ данни: Лице или организация, която обработва лични данни от името на администратора.

3.3. Облачни услуги: Услуги за съхранение, обработка и достъп до данни чрез интернет, предоставяни от външен доставчик, включително SaaS, PaaS и IaaS модели.

3.4. Технически мерки: Средства за защита на личните данни чрез технологии, включително криптиране, автентикация и контрол на достъпа и др.

3.5 Организационни мерки: Политики, процедури и процеси, които осигуряват съответствие с изискванията за защита на личните данни.

Значението на всички останали термини в настоящата Политика следва да бъде съгласно съответния контекст и приложимото законодателство.

Принципи на обработка на лични данни

Член 4: Основни принципи

4.1. Законосъобразност, добросъвестност и прозрачност: Личните данни се обработват в съответствие със закона, добросъвестно и прозрачно спрямо субектите на данни.

4.2. Ограничение на целите: Данните се събират и обработват само за конкретни, изрично указани и легитимни цели.

4.3 Минимализиране на данните: Обработват се само данните, необходими за съответната цел.

4.4 Точност: Личните данни се поддържат точни и, когато е необходимо, актуализирани.

4.5. Ограничение на съхранението: Данните се съхраняват за период, не по-дълъг от необходимото за целите на обработката.

4.6. Цялостност и поверителност: Данните се защитават срещу неразрешена или незаконна обработка чрез подходящи технически и организационни мерки.

4.7. Отчетност: ВАдвС носи отговорност за спазването на тези принципи и е готов да докаже съответствие с тях.

Технически и организационни мерки

Член 5: Прилагани технически и организационни мерки

Раздел 5.1: Технически мерки

5.1.1 Доставчиците на облачни услуги, използвани от ВАдвС следва да използват поне някой от следните механизми за криптиране на данни или такива, предоставящи по-високо ниво на сигурност:

- **При съхранение:** Данните се криптират с помощта на AES-256 алгоритъм;
- **При пренос:** Използване на TLS (Transport Layer Security) протоколи за сигурна комуникация;
- **Ключове за криптиране:** Управление на ключове чрез защитени хранилища и редовна ротация.

5.1.2 Доставчиците на облачни услуги следва да предоставят на ВАдвС възможност за осъществяване на контрола на достъпа чрез следните механизми:

- Използване на двуфакторна автентикация за всички потребители с достъп до чувствителни данни.
- Ограничаване на достъпа до данни на база роля (Role-Based Access Control - RBAC).
- Редовен преглед на правата за достъп и премахване на ненужни права.

5.1.3 Доставчиците на облачни услуги следва да предоставят на ВАдвС възможност за Мониторинг и логване чрез:

- Централизирана система за логване на всички дейности, свързани с достъп до данни.
- Автоматизирани инструменти за откриване на аномалии и сигнали за потенциални заплахи.
- Запазване на логовете за минимум 12 месеца.
- Възможност за ВАдвС да интегрира собствени софтуерни продукти, позволяващи осигуряването на адекватно ниво на защита.

5.1.4 Доставчиците на облачни услуги, използвани от ВАдвС, следва да предоставят или да позволяват на ВАдвС да интегрира защита срещу злонамерен софтуер по някои от следните начини или по други начини, осигуряващи по-високо ниво на защита:

- Инсталиране на антивирусни и анти-зловредни програми на всички устройства.
- Редовно сканиране за уязвимости и злонамерен софтуер.

- Блокиране на подозрителни IP адреси и мрежови връзки.

5.1.5 Доставчиците на облачни услуги, използвани от ВАдвС, следва да предоставят или да позволяват на ВАдвС да прилага мерки по съхранение и възстановяване при непредвидени събития, които включват, но не се ограничават до:

- Автоматично създаване на резервни копия на данните поне веднъж дневно.
- Съхранение на резервните копия в защитени и географски разпределени хранилища.
- Провеждане на регулярни тестове за възстановяване на данни.

Раздел 5.2: Организационни мерки

5.2.1 Доставчиците на облачни услуги, използвани от ВАдвС, както и ВАдвС следва да приемат, прилагат и редовно да актуализират политики и процедури, а именно:

- Създаване на вътрешни политики за защита на личните данни, включително правила за достъп, съхранение и изтриване.
- Регулярно актуализиране на политиките в съответствие с промените в законодателството.
- Планове за действие при инциденти, свързани с нарушаване на сигурността.

5.2.2 ВАдвС осъществява периодични и извънредни обучения на своите служители, работещи с облачни услуги, както и предприема периодични кампании за осведоменост на своите потребители, които включват:

- Провеждане на редовни обучения за служителите относно защита на личните данни и информационна сигурност.
- Предоставяне на насоки за разпознаване на фишинг атаки и други заплахи.
- Организиране на симулации на инциденти за тестване на готовността на екипа.

5.2.3 При избор на доставчици на облачни услуги ВАдвС:

- Изисква от доставчиците на доказателства за съответствие със стандартите за сигурност (напр. ISO 27001).
- Включва на клаузи за защита на личните данни в договорите с доставчици.
- Извършва редовен одит и мониторинг на практиките на доставчиците на облачни услуги.

5.2.4 ВАдвС осъществява редовен преглед и оценка като извършва поне следните действия:

- Провеждане на периодични одити за оценка на съответствието с приетите мерки.
- Преглед на резултатите от тестове за сигурност и внедряване на препоръки за подобрение.
- Актуализиране на мерките въз основа на нововъзникнали заплахи и технологии.

Управление на инциденти

Член 6: Процедура за управление на инциденти

Раздел 6.1: Откриване и докладване на инциденти

6.1.1 Всички служители, доставчици и партньори са длъжни незабавно да докладват на длъжностното лице по защита на данните и на председателя на ВАдвС за инциденти, свързани с лични данни.

6.1.2 Инцидентите се регистрират в централизирана система за управление на инциденти, като се документират следните данни:

- Дата и час на откриване на инцидента.
- Засегнати системи и вид на компрометираните данни.
- Потенциални причини за инцидента.
- Идентифицирани рискове за субектите на данни.
- Предприети мерки за преустановяване на инцидента (когато е продължаващ) и предприети мерки за ограничаване на ефектите от инцидента.
- Оценка за необходимостта от уведомяване на компетентния надзорен орган и засегнатите субекти на данните

Раздел 6.2: Оценка и класификация на инциденти

6.2.1 Всеки инцидент се оценява по степен на риск за субектите на данни.

6.2.2 Инцидентите се класифицират по следните нива:

- **Нисък риск:** Без съществено влияние върху правата и свободите на субектите.
- **Среден риск:** Може да доведе до временни затруднения за субектите.
- **Висок риск:** Сериозно влияние върху правата, свободите или поверителността на субектите.

Раздел 6.3: Реакция и смекчаване

6.3.1 Във ВАдвС се създава се екип за управление на инциденти, който включва най-малко следните лица: Длъжностното лице по защита на данните, председателя на ВАдвС, Главния секретар на ВАдвС и специалист по информационна сигурност. По преценка на председателя на ВАдвС, отчитайки спецификите на всеки отделен инцидент, могат да бъдат ангажирани и външни консултанти независимо от тяхната експертиза – юридическа, технологична, връзки с обществеността и т.н.

6.3.2 Предприемат се незабавни мерки за ограничаване на въздействието на инцидента, включително:

- Изолиране на засегнатите системи.

- Промяна на пароли и ограничаване на достъпа.
- Уведомяване на засегнатите потребители и предоставяне на инструкции за защита.
- Изясняване на произхода на инцидента – дали е от действия на служители или доставчици на ВАдвС или от самия доставчик на облачни услуги;
- Свързване с представители на доставчика на облачни услуги и координиране на стратегия за преустановяване на инцидента и ограничаване на въздействието от него

Раздел 6.4: Уведомяване на надзорните органи и субекти на данни

6.4.1 ВАдвС следва да осигури гаранции, че при инцидент, за който не може да разбере чрез своя достъп до облака, ще бъде информиран от доставчика на облачни услуги незабавно.

6.4.2 При инциденти с висок риск, ВАдвС уведомява компетентния надзорен орган в рамките на до 72 часа от откриването на инцидента.

6.4.3 Засегнатите субекти на данни се уведомяват незабавно, като се предоставя следната информация:

- Естество на инцидента.
- Предприети мерки за защита на данните.
- Препоръки за действия от страна на субектите на данни.

Раздел 6.5: Документация и преглед

6.5.1 Всички инциденти се документират, включително предприетите действия и изводите от разследването.

6.5.2 Провежда се анализ след инцидента за идентифициране на слабости и подобряване на мерките за сигурност.

6.5.3 Резултатите от анализа се представят на ръководството и се използват за актуализация на политиките и процедурите.

Избор на доставчици на облачни услуги

Член 7: Процедура за избор на доставчици на облачни услуги

Раздел 7.1: Подготовка за избор

7.1.1 При подготовката за избор на доставчици на облачни услуги ВАдвС следва да определи нуждите и изискванията към тях като извърши поне следните действия:

- Идентифициране на целите и спецификите на обработката на данни.
- Оценка на обема, вида и чувствителността на данните.

- Изготвяне на технически и функционални спецификации или съобразяване дали предлаганите от съответния доставчик спецификации отговарят на нуждите и изискванията на ВАдвС (когато се планира използването на SaaS).

Раздел 7.2: Оценка на потенциалните доставчици

7.2.1 ВАдвС прилага следните критерии за оценка на евентуалните доставчици на облачни услуги:

- Репутация и опит на доставчика в областта на облачните услуги.
- Способности за осигуряване на съответствие с ОРЗД и приложимите закони в областта на защитата на данните.
- Наличие на сертификации като например: ISO 27001, SOC 2 и др.
- Технически мерки за защита на данните, включително криптиране и автентикация.
- Условия за непрекъснатост на услугите и възстановяване при аварии.
- Използване на “Privacy by design” или “Privacy by default”;

Раздел 7.3: Договорни изисквания

7.3.1 С всеки доставчик на облачни услуги освен договор за самата слуга следва да се сключи и договор за обработка на лични данни съгласно чл. 28 от ОРЗД. Основни елементи на тези договори освен задължителното съдържание съгласно чл. 28 от ОРЗД са:

- Подробно описание на предоставяните услуги.
- Установяване на отговорности за сигурността на данните.
- Задължения за уведомяване при инциденти със сигурността.
- Разпоредби за подобработващи данни, включително предварително одобрение от ВАдвС.
- Условия за прекратяване на договора и връщане или изтриване на данните.

Раздел 7.4: Одит и мониторинг

7.4.1 Процедури за одит:

- ВАдвС следва да извършва периодични проверки за съответствие с договорните изисквания.
- ВАдвС трябва да има достъп до записи на дейности и отчети за сигурността.
- Доставчиците на облачни услуги трябва да осигуряват провеждане на независими одити при необходимост.

7.4.2 ВАдвС следва да може да извършва мониторинг на предоставяните услуги, който включва, но не се ограничава до:

- Използване на инструменти за наблюдение на производителността и наличността.
- Постоянна оценка на рисковете и внедряване на мерки за тяхното управление.

Заключителни разпоредби

За неуредени въпроси се прилагат Вътрешните правила на Висш адвокатски съвет
за мерките за защита на личните данни съгласно Регламент 2016/679.

Настоящата политика е задължителна за всички служители, партньори и доставчици, свързани с дейността на Организацията. Нарушенията на тази политика могат да доведат до налагането дисциплинарни наказания (включително дисциплинарно уволнение), както и дължимост на обезщетения за причинени вреди съгласно общото законодателство в Република България.

Председателят на ВАдвС и длъжностното лице по защита на данните осъществяват контрол по изпълнението, прилагането и спазването на настоящата политика.

ПРЕДСЕДАТЕЛ НА ВИСШИЯ
АДВОКАТСКИ СЪВЕТ: /п/
АДВ. Д-Р ИВАЙЛО ДЕРМЕНДЖИЕВ