|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Версия** | **Дата** | **Описание** | **Автор** | **Одобрил** |
|  |  |  |  |  |

1. Предназначение на процедурата

Тази процедура регламентира взаимоотношенията между ПАТО ЕООД и всички външни контрагенти, които обработват лични данни от негово име (подизпълнители). Тези лица се явяват в ролята на „обработващ лични данни“ по смисъла на ОРЗД.

1. Нормативна уредба

* [Член 4, точка 8](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art4) и [член 28](https://web.apis.bg/e.php?celex=32016R0679&ToPar=Art28) от Общия регламент за защита на данните (ОРЗД)

1. Задължения и роли

Длъжностното лице по защита на данните / Отговорникът по защита на данните отговаря за одобряването на избора на подизпълнители, които обработват лични данни в съответствие с изискванията на тази процедура, както и за последващото извършване на редовни проверки на извършвана от тях дейност.

Лицата, които имат взаимоотношения с такива подизпълнители, трябва да гарантират, че цялата външна дейност по обработката на данни е възложена в съответствие с настоящата процедура.

Представителят на IT-отдела отговаря за осигуряването на подходящи технически и други ресурси, които биха могли да бъдат необходими и да подпомогнат Длъжностното лице по защита на данните / Отговорника по защита на данните в процеса на наблюдение и управление на дейността.

1. Ход на процедурата
2. ПАТО ЕООД избира само доставчици, които могат да осигурят техническа, физическа и организационна сигурност и които отговарят на поставените изисквания по отношение на всички лични данни, които ще обработват.

Главният счетоводител редовно извършва преглед на всички договори, за да провери дали се обработват лични данни. Тези проверки се извършват, дори ако дейността по обработка на лични данни не е основната причина за сключване на договора.

ПАТО ЕООД гарантира, че всички мерки за сигурност са посочени в договора с външния изпълнител, който обработва лични данни.

1. Доставчици от страни извън ЕС могат да бъдат избрани само при положение, че е изпълнено едно от следните специфични условия, изисквани в допълнение към останалите условия, посочени в тази процедура:

* ако доставчикът или държавата, в която пребивава или е установен, са били идентифицирани като осигуряващи адекватно ниво на защита на личните данни в решение за адекватност от страна на Европейската комисия, или
* ако са налични задължителни фирмени правила за предаване на данни извън ЕС установени между ПАТО ЕООД и доставчика, за да се гарантират правата на субектите, и тези правила са одобрени от надзорния орган (за България това е Комисията за защита на личните данни), или
* когато споразумението с доставчика е одобрено от надзорния орган.

1. Преди да бъде ангажиран външен доставчик, се извършва оценка на въздействието върху защитата на данни (ОВЗД), като се вземат предвид техническите и организационни мерки за сигурност. ОВЗД по отношение на доставчиците се извършва в съответствие с изискванията на Процедура за оценка на въздействието върху защитата на данните (GDPR\_PROC\_10) и използваната отПАТО ЕООД методология за ОВЗД.
2. Ако Длъжностното лице по защита на данните / Отговорникът по защита на данните счете за необходимо (например, поради завишени изисквания по отношение защитата на чувствителни лични данни), преди сключването на договора може да се извърши одит на системите за сигурност на доставчика съгласно изискванията на одобрени фирмени правила или стандарти за сигурност.
3. ПАТО ЕООД сключва писмено споразумение с подизпълнителя за предоставяне на възложената услуга и изисква от контрагента да осигури подходящи мерки за сигурност на личните данни, които ще обработва. За целта в споразумението се предвиждат съответни гаранции, като например:

* Забрана доставчикът да използва от своя страна подизпълнители за обработката на личните данни без изрично писмено разрешение от ПАТО ЕООД. Когато ПАТО ЕООД разреши на доставчика да превъзложи обработката на лични данни на подизпълнител, доставчикът от първо ниво трябва да забрани на подизпълнителя от второ ниво (и по-нататък по веригата) да превъзлага дейността по обработка на данни на подизпълнители без писменото разрешение на ПАТО ЕООД;
* Договорите с подизпълнители от второ ниво се одобряват, само ако изискват от тях да спазват най-малко същите разпоредби за сигурност и другите изисквания, които се отнасят и до основната организация подизпълнител (доставчик). При прекратяването на договор с подизпълнител на второ и следващо ниво, съответните лични данни трябва да бъдат унищожени или върнати на ПАТО ЕООД по веригата от подизпълнители;
* Право на (ПАТО ЕООД да извършва редовни проверки на системите за сигурност на доставчика през периода, в който той има достъп до личните данни.