Наръчник
по защита на личните
данни

RAVENA
SECURITY SYSTEMS

Съдържание

Описание

РАВЕНА ООД, като Администратор на ЛД, събира и обработва ЛД във връзка с предмета на дейностите си в областта на GPS – проследяване на обекти, събиране и обработване на телеметрични данни, внос и продажба на електронни устройства, застраховане, услуги в Студио за красота, внос и продажба на козметични продукти, обучения, издаване на удостоверения.
Личните данни се обработват и във връзка с трудовите правоотношения на служителите, както и при сключване на граждански договори.

Прилага се Система за защита на ЛД (СЗЛД) – това е набор от политики, правила, технически и правни процедури, описващи техническите и организационни мерки, предприемани за защита на ЛД при тяхната обработка.

Този Наръчник по защита на личните данни съдържа синтезирано описание на дейностите при обработката на ЛД, които АЛД прилага в ежедневната си дейност. Може да се използва и за запознаване на служителите с приетите правила за работа. Съдържат се препратки към използваните документи. Всички документи по защита на ЛД, които се цитират по-надолу се съхраняват от АЛД и са на разположение при поискване в хартиен или електронен формат.

Основни документи

Списък на основните документи, които АЛД - РАВЕНА ООД използва за информиране относно взетите мерки за изпълнение изискванията на Регламент (ЕС) 679/2016

Политики

Политика за защита на личните данни – обща за всички дейности на дружеството
Политика сайт ravena.bg
Политика сайт skywatch.bg
Политика сайт evasereva.com и esmakeupstudio.com

Декларации по GDPR за служители

Декларация информираност - служители
Декларация – запознат
Декларация за поверителност (оправомощен служител за обработка на ЛД)

Заповеди

Заповед за утвърждаване на Политика за защита на личните данни

Примери за най-често приложение на Основните документи:

1. **При назначаване на нов служител се предоставят следните документи:**
   1.1 Политика за защита на личните данни – обща за всички дейности
   1.2 Декларация информираност - служители
   1.3 Декларация – запознат
   1.4 Декларация за поверителност (оправомощен) – тази декларация се подписва от всеки служител, който обработва ЛД
   1.5 Всеки служител се запознава и със Заповед за утвърждаване на Политика за защита на личните данни

Забележка:*Подписаните Декларация – запознат и Декларация за поверителност (оправомощен) се съхраняват в досието на всеки служител.*

2. **Служители, назначени към момента на внедряване на СЗЛД:**
   2.1 Политика за защита на личните данни – обща за всички дейности

2.2 Декларация информираност - служители
2.3 Декларация – запознат
2.4 Декларация за поверителност (оправомощен) – тази декларация се подписва от всеки служител, който обработва ЛД
2.5 Всеки служител се запознава и със Заповед за утвърждаване на Политика за защита на личните данни

Забележка: *Декларацията по т.2.3 се предоставя при условие, че няма вече подписана такава до момента.*

3. **Документи за сайтове:**
   3.1 Политика сайт ravena.bg
   3.2 Политика сайт skywatch.bg
   3.3 Политика сайт evasereva.com и esmakeupstudio.com

Забележка: *Политиките се публикуват на съответните сайтове в специално отделени лесно достъпни секции.*

Права на субектите на данни

Съгласно Общ Регламент (ЕС) 2016/679, Администраторът на лични данни предприема необходимите мерки за предоставяне на всякаква информация, свързана с правата на физическите лица.

При получаване на законово искане от субект на данните към АЛД се изпълняват съответните процедури, заложени в СЗЛД.

Всяка процедура от СЗЛД се състои от описателна част, отговорници, действия и форми(бланки), които документират процедурата за изпъление искането на субекта на данни. Процедурите имат вграден Механизъм за контрол, чрез който се следи и гарантира правилността на изпълнението.

За всяко право има разписана Правна процедура и съответните бланки на документи, които се намират в края на всяка процедура.
Пример:
Субектът на данни упражнява *Право на информация и достъп*

- *от СЗЛД се намира Процедура ППЗЛД Б 03.01* - Право на информация и достъп
  - *Субектът попълва форма "ИСКАНЕ ЗА ДОСТЪП НА СУБЕКТА ДО ДАННИТЕ СИ"- **Форма Б03_01***

- *С форма „УВЕДОМЛЕНИЕ ЗА ОБРАБОТВАНИ ЛИЧНИ ДАННИ“, РАВЕНА ООД уведомява субекта за резултата - **Форма Б03_02***
- *Ако искането е неоснователно с форма „ОТКАЗ ЗА ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ ЗА ОБРАБОТВАНИ ЛИЧНИ ДАННИ“, се прави отказ за предоставяне на исканата информация и се описват причините за отказа - **Форма Б03_03***
- *Всяко действие се отразява в РЕГИСТЪРА НА ИСКАНИЯТА*

Аналогични са действията при постъпване и на другите видове искания, като се използват съответните процедури:

- Право на информация и достъп - *Процедура ППЗЛД Б 03.01*
- Право на корекция на данните - *Процедура ППЗЛД Б 04.01*
- Право на изтриване на данните - *Процедура ППЗЛД Б 05.01*
- Право на ограничаване на обработката на данни - *Процедура ППЗЛД Б 06.01*
- Право на преносимост на данните - *Процедура ППЗЛД Б 07.01*
- Право на възражение - *Процедура ППЗЛД Б 08.01*
- Право на подаване на жалба до надзорния орган - *Процедура ППЗЛД Б 09.01*

Забележка: Срокът за отговор на исканията е един месец.

Съгласие

Случаите, когато за обработката на ЛД е необходимо да се получи съгласието на субекта на данните са описани в правната процедура от СЗЛД - СЪГЛАСИЕ, СВЪРЗАНО С ОБРАБОТКАТА НА ЛИЧНИ ДАННИ - ППЗЛД Б 01.01.

Когато обработването се извършва въз основа на съгласие, АЛД трябва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни. За съгласието се използват формите:

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ - (**Форма Б01_01**)

ДЕКЛАРАЦИЯ ЗА ОТТЕГЛЕНЕ НА СЪГЛАСИЕ - (**Форма Б01_02**)

ДЕКЛАРАЦИЯ ЗА ЧАСТИЧНО ОТТЕГЛЕНЕ НА СЪГЛАСИЕ - (**Форма Б01_03**)

Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законо-съобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде

съгласие, субектът на данни бива информиран за това. Оттеглянето на съгласие е също толкова лесно, колкото и даването му.

Пример:
Не е необходимо АЛД - РАВЕНА ООД да получи съгласие за обработка на ЛД при сключване на трудови и граждански договори.
Изрично съгласие, обаче е необходимо за обработката на специалните категории лични данни при някои от услугите в козметичния център. Могат да се използват например формите от СЗЛД - СЪГЛАСИЕ-МИКРОБЛЕЙДИНГ, СЪГЛАСИЕ-СНИМКИ-СТУДИО ЗА КРАСОТА, REMOVAL ДЕКЛАРАЦИЯ.

Договори с клиенти - SKYWATCH

Всеки **договор с клиент** съдържа и условията за спазване на изискванията на GDPR. Тези условия представляват СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ към основния договор за предоставяне на неизключително право на ползване на програмен продукт, услуга и др., когато изпълнението на договора е свързано с обработка на ЛД.

Договорите с клиенти са относно правото на ползване на Софтуер за проследяване на GPS координати – SKYWATCH. Поради спецификата на системата в тези случаи РАВЕНА ООД и клиента са съвместни администратори на лични данни, съгласно изискванията на Регламент (ЕС) 2016/679. Всеки от АЛД носи собствена отговорност при обработката на ЛД. При подписването на нов договор се използва се форма **СПОРАЗУМЕНИЕ АЛД-АЛД.** За всички вече съществуващи основни договори, чието действие не е прекратено, **СПОРАЗУМЕНИЕ АЛД-АЛД**, е необходимо да се добави.

Договори АЛД-ОЛД

Когато обработването се извършва от името на даден администратор, администраторът използва обработващи лични данни (ОЛД). Обработването се урежда с договор или с друг правен акт. РАВЕНА ООД използва договори с ОЛД в следните случаи:

1. Управление на човешките ресурси и Финансово-счетоводна дейност
2. Външни услуги на IT
3. СТМ

4. Други, които имат достъп до ЛД, обработвани от АЛД

С всеки отделен ОЛД се сключва СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ към основния договор при подписването на нов или се добавя към съществуващия. Използва се форма **СПОРАЗУМЕНИЕ АЛД-ОЛД.**

Предаване на данни на трети страни

За информация, когато се наложи предаване(трансфер) на ЛД на европейски граждани в страни извън ЕС и ЕИП е следното описание относно ЗЛД:

Към настоящия момент (м.11.2018), ЕК е признала следните държави извън ЕС и ЕИП с адекватно ниво на защита: САЩ (ограничено в рамките на Privacy Shield), Нова Зеландия, Източна Република Уругвай, Израел, Андора, Фарьорските острови, Джърси, остров Ман, остров Гърнзей, Аржентина, Швейцария. В момента тече процедура на преговори между ЕС и Япония за признаване на адекватно ниво на защита при условията на реципрочност.

Предаването на лични данни на трета държава или международна организация се осъществява при отчитането на съответното адекватно ниво на защита за тази държава или международна организация. Информация за осигуряването на адекватното ниво на защита на съответната държава може да бъде намерено на следните адреси на сайта на ЕК: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en.

В случаите, при които РАВЕНА ООД е необходимо да предава лични данни на държави, които не са в списъка на ЕС за адекватност, е необходимо да се въведат подходящи гаранции за защита правата на субектите на данните чрез:

1. Наличието на правообвързващо споразумение;
2. Обвързващи фирмени правила;
3. Стандартни клаузи за защита;
4. Одобрен кодекс за поведение;
5. Одобрен механизъм за сертифициране.

При липса на решение относно адекватното ниво на защита и на подходящи гаранции, предаването или съвкупността от предавания на лични данни на трета държава или международна организация се извършва само при едно от следните условия:

1. субектът на данните е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за субекта на данните поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции;
2. предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
3. предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
4. предаването е необходимо поради важни причини от обществен интерес;
5. предаването е необходимо за установяването, упражняването или защитата на правни претенции;
6. предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
7. предаването се извършва от регистър, който съгласно правото на Съюза или правото на държавите членки е предназначен да предоставя информация за обществеността и е достъпна за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

Ако не са налице горепосочените условия, предаването на данни на трета държава или международна организация може да се извършва само ако предаването не е повторяемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите законни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни.

Технически мерки за защита

Техническите мерки се осъществяват с цел предотвратяване изтичане на информация, отнасяща се до ЛД на физическите лица.
Мерките при защита на ЛД на **хартиен носител са:**

- монтирани са ключалки на шкафовете, където се съхраняват хартиените носители с ЛД;
- до всички помещения има контрол на физическия достъп – всеки посетител се придружава от служител на АЛД до определените помещения;
- охрана и система за сигурност /СОТ в помещенията на сградите/;
- всички досиета и данните, за които е изтекъл срокът за съхранение са унищожени или върнати на притежателя.
- не се съхраняват копия на лични документи (лични карти, международни паспорти и др.) без поискано съгласие за това. Всяко копие на документ, за който няма съгласие трябва или да се върне на притежателя или да бъде унищожено.
- досиетата с ЛД се съхраняват в заключени шкафове в отделно помещение.
- трудови досиета на работници или служители и документите, които удостоверяват осигурителен стаж и осигурителен доход, се съхраняват за срок, не по-малък от 50 години.

След изтичане на съответните срокове хартиените носители се унищожават съгласно процедурата за унищожаване на данни - ТПЗЛД А 04.01 (А.4.3.2).

Мерките при защита на ЛД в **електронен формат и комуникации** са:

1. Достъпът до всякакъв вид информация в електронен формат се осъществява със съответните потребителски права.
2. Достъпът до всеки компютър в офиса е ограничен с потребителско име и парола. За прилагане на съответните мерки се използва процедура „КОНТРОЛ НА ДОСТЪПА“ - ТПЗЛД А 05.01.
3. Съхранението на лични документи става само със съгласието на субектите на данните и файловете, които се намират върху компютрите, са защитени.
   Файловете, които съдържат ЛД се намират на специално отделена част от дисковото пространство на всеки локален компютър (директория на логически диск D:\). Тази част е криптирана и всеки потребител получава ключа за достъп, в зависимост от длъжността си.

Не се разрешава обработката на файлове с ЛД извън тази обособена на всеки локален компютър част.

Регламент 2016/679 изисква използване на технологии, с които да се прилага сигурна защита на ЛД – напр. криптиране, псевдонимизация или други. В Регламента няма точни правила за изпълнението на това изискване. Подходът може да бъде разгледан в техническа процедура „КРИПТОГРАФИЯ“ ТПЗЛД А 06.01. Криптографските ключове и конкретната технология се определят от този, който извършва криптирането. За тази цел може да се използват например вградените функции на ОС на компютрите, външна специализирана програма и др. Решението за използване на конкретна технология се взима от ръководството по предложение на отговорните за ИТ поддръжката лица.

4. Архивирането на файловете се извършва на външно устройство и/или облак – начина, средствата и процедурите на архивиране и възстановяване на данните са задължение на отговорните за ИТ поддръжката лица.
5. В случаи изискващи трансфер на ЛД чрез имейл, следва личните данни да се изпращат чрез технологии за сигурна защита на изпращаната информация. Всеки служител е обучен и спазва правилата за работа с използваната текуща технология.
6. Описанието на изградената мрежова инфраструктура, споделените ресурси, регламентираните достъпи, потребителите, паролите са описани подробно и се съхраняват в запечатани пликове в заключен шкаф с ограничен достъп. Подробно описание на мерките се намира в Техническа процедура - КОНТРОЛ НА ДОСТЪПА - ТПЗЛД А 05.01.
7. Операционните системи на локалните компютри и използваните софтуерни продукти са актуализирани до последните версии на производителите. Този процес е автоматизиран и настроен за изпълнение без намеса на потребителите.
8. При необходимост от изнасяне на активи – напр. преносими компютри, външни памети с информация и др. се спазват правилата, описани в Техническа процедура ФИЗИЧЕСКА СИГУРНОСТ И СИГУРНА СРЕДА ОТНОСНО ЗЛД ТПЗЛД А 07.01.
9. Забранено е предоставяне на комютъра на трети лица.
10. При необходимост от извършване на ремонт на комютърна система трябва да се спазват следните правила:
    - достъпът на сервизното лице е през специално създаден профил, с права само върху системната част и без права и ключове върху специалната част с файлове с ЛД;

- при необходимост от изнасяне на PC от офиса дисковете с информация трябва да бъдат свалени. Ако това не е възможно, файловете с ЛД трябва да бъдат унищожени.

11. Забранено е изпращане на лични данни чрез социални мрежи: Фейсбук, Месинджър, Вайбър и други.
12. Забранява се сваляне и инсталиране на приложения различни от работните.
13. Използва се надежден, лицензиран антивирусен софтуер.
14. Сигурност на комуникациите:

14.1 Технически механизъм:

- Периодично обновяване на фърмуера и софтуера върху всички устройства управляващи комуникационната мрежа;
- Отдаленият достъп до всички устройства е контролиран и се извършва съгласно сключени договори с външен изпълнител или служител. Описание на правилата за работа се намира в ОРГАНИЗИРАНЕ НА СИГУРНОСТТА И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ - **ТПЗЛД А 02.01**, **А.2.2 МОБИЛНИ УСТРОЙСТВА И РАБОТА ОТ РАЗСТОЯНИЕ**
- Достъпът до вътрешни ресурси, чрез защитната стена е разрешен чрез ползването само на следните услуги, респективно комуникационни портове: HTTP (80,81), HTTPS (443), SMTP (25), SMTPS (587), IMAP (143), DNS (53) и SSH (22);

14.2 Физически механизъм:

Комуникационното оборудване (маршрутизатори, комутатори, и пр.) и дистрибуторните панели са разположени в обособени места с контролиран достъп до тях.

14.3 Достъпът до ресурсите на изградената система за безжични комуникации в инфраструктурата на организацията е регламентиран и спазва правилата описани СИГУРНОСТ НА КОМУНИКАЦИИТЕ - **ТПЗЛД А 09.01.**

15. Вземайки предвид изискването на Регламента и с цел запазване на функционалността и подобряване на защитата и сигурността на данните за софтуерната система SKYWATCH се прилага криптиране само на част от БД съдържаща ЛД (таблици). За всички останали таблици тази технология не е наложителна за прилагане.
16. При отстраняването на инцидентите в системи на дистрибуторите на SKYWATCH, АЛД заедно с дистрибутора договарят ред на действията. Това е описано в специално приложение, анекс или друг вид споразумение към основния договор, в което да се регламентира напр. получаването на временна парола за достъп за времето на

отстраняването на ицидента, ангажираност за непредаване, получаване, копиране на данни и др.

Организационни мерки за защита

Организационните мерки предприети от АЛД са част от общата система за защита на ЛД.
Основните организационни мерки са: определени са зоните с контролиран достъп; определени са помещенията, в които ще се обработват лични данни; определени са помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; определена е организацията на физическия достъп; определени са използваните технически средства за физическа защита.

1. Обучението на участниците в процесите по обработка на лични данни за правата, задълженията и отговорностите въведени с GDPR е постоянно задължение на АЛД. За да се защитят събраните, съхраняваните и обработваните от организацията лични данни, е важно служителите и другите заинтересовани страни, участващи в осигуряването на ефективна защита на данните, да имат необходимите компетенции. Обучението се извършва периодично и може да бъде вътрешно или външно. Процедура СИГУРНОСТ НА ЧОВЕШКИТЕ РЕСУРСИ **ТПЗЛД А 03.01** може да се използва за създаване на съответната организация.
2. Документите от раздел ОСНОВНИ ДОКУМЕНТИ трябва да бъдат на разположение и представяни при поискване. Всички служители се запознават с тях и подписват съответните декларации, че са запознати и информирани.
3. При назначаване на новопостъпили служители или при служители, на които се налага промяна на правата за достъп до информационни ресурси може да се използва техническа процедура „ОРГАНИЗИРАНЕ НА СИГУРНОСТТА И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ“ **ТПЗЛД А 02.01** - ФОРМА 02_01 - Заявка за достъп.
4. Сигурност на човешките ресурси – ***Процедура ТПЗЛД А 03.01***
   Всички служители, подписват Декларация за конфиденциалност преди да получат достъп до средствата за обработка на информация в организацията.
   4.1 При назначаване на нов служител се изпълнява т.1 от Основни документи

4.2 При напускане на служител, трябва да бъдат спазени ангажиментите по отношение на сигурността. Да бъдат върнати всички активи (компютри, мобилни устройства и др.), които съдържат лични данни със съответен приемо-предавателен протокол. Да бъдат сменени всички пароли за достъп до системите. (СИГУРНОСТ НА ЧОВЕШКИТЕ РЕСУРСИ - **ТПЗЛД А 03.01**)

5. При подписване договор с клиент се подписва и СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ.
6. В Техническа процедура УПРАВЛЕНИЕ НА ОПЕРАЦИИТЕ **ТПЗЛД А 08.01** са определени реда, отговорностите, както и системата от мерки, способи и средства за осигуряване на подходящо ниво на защита и ефективен контрол на физическата сигурност на работната среда за недопускане или намаляване до минимум на щетите от произшествия свързани с обработка и защита на ЛД.

Унищожаване на данни

След изтичане на съответните срокове за съхранение при обработката на ЛД, всички данни от съответните носители трябва да се унищожат. в Техническа процедура УПРАВЛЕНИЕ НА ФИРМЕНИТЕ АКТИВИ - ТПЗЛД А 04.01 (А.4.3.2) са описани начините, способите и средствата за унищожаване на носители по сигурен начин, когато не са необходими вече или срокът за обработка е изтекъл.

Фирмени активи с ЛД – това са компютри, архивиращи устройства, мобилни устройства, хариени носители и др., на които се съхраняват лични данни.

Сроковете за обработка на ЛД за всяка дейност и регистър са описани в **РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТКА.**

Нарушение на сигурността

Организационните и техническите мерки, които АЛД предприема за недопускане или намаляване до минимум на щетите от произшествия и инциденти със сигурността на ЛД са описани в две процедури от СЗЛД.

1. Техническата процедура УПРАВЛЕНИЕ НА ИНЦИДЕНТИ ПО ОТНОШЕНИЕ СИГУРНОСТТА НА ДАННИТЕ НА ФИЗИЧЕСКИ СУБЕКТИ - **ТПЗЛД А 10.01** определя реда и отговорностите при управлението на инциденти, свързани със сигурността при обработката на ЛД.
   Описани са дейностите, отговорностите и подхода при управлението на инцидентите в сигурността. Различните типови инциденти и съответните реакции преди по време и след инцидентие, както и тяхното документиране довеждат до намаляване на риска при обработката на ЛД.
   Ако бъде установена потенциална или реална уязвимост/слабост или пропуск, които могат да компрометират сигурността, обработващия служител веднага уведомява прекия си Ръководител. Документира се с попълване на **Форма 10_01** (Доклад за възникване на слабости или инцидент).

2. В случай на нарушение на сигурността и установяване на изтичане на информация за обработваните ЛД се прилага Правна процедура НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ - ***ППЗЛД Б 10.***
   При установяване на нарушение в сигурността на личните данни, се уведомява надзорния орган (КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ) - **Форма Б10_01**.

   Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, РАВЕНА ООД, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни - **Форма Б10_02**.

   Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне, но не по-късно от 72 часа след като е забелязано нарушението.

Регистри

1. **РЕГИСТЪР НА ДАЙНОСТИТЕ ПО ОБРАБОТВАНЕ**

   Всеки АЛД поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа обощена информация за обработването на лични данни от организацията. Представянето на регистъра е в табличен вид. В него за всеки вид дейност се описват данни като: целите на обработването, описание на категориите субекти на данни и на категориите лични данни, категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации и др.

2. **РЕГИСТЪР НА ИСКАНИЯТА**

   Регистърът служи за документиране на предприетите действия от АЛД при изпълнение на законовите си задължения относно исканията на субектите на данни.

3. **РЕГИСТЪР НА ЖАЛБИТЕ**

   Правната процедура ПРОЦЕДУРА ПРИ ОПЛАВАНИЯ, ЖАЛБИ И СИГНАЛИ ОТ СУБЕКТА **ППЗЛД Б 09.01** определя реда и отговорностите на АЛД РАВЕНА ООД, относно задължението да получи и обработи жалбата на субекта на личните данни, относно следните му права:

   - Жалба срещу взети решения при подадени искания до АЛД за достъп, корекция, изтриване, ограничаване на обработката, възражения, пренос на данни.
   - Жалби относно начина на разглеждане на искания от страна на субекта

   Процедурата обхваща целия процес, свързан с правото на субекта да подаде жалба при несъгласие с начина, по който се обработват личните данни, които го засягат и които той е предоставил на РАВЕНА ООД, в качеството на Администратор на лични данни.

   Документирането на процеса по обработване на жалбите се отбелязва в Регистър на жалбите, представен в табличен вид.