ПРИЛОЖЕНИЕ № 1

Общо описание
на
Специализирана автоматизирана информационна система за поддържане на регистрите в КЗЛД, в изпълнение изискванията на новата правна рамка

1. Общи изисквания към системата

Комисията за защита на личните данни (КЗЛД) поддържа следните регистри:

Публични регистри:

- Регистър на длъжностните лица по защита на данните;
- Регистър на акредитирани сертифициращи организации;
- Регистър на кодекси за поведение.

Непублични:

- Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия (Регистър на нарушенията и предприетите мерки).

Регистрите се поддържат с помощта на специализирана автоматизирана информационна система (САИС).

Общи изисквания към САИС:

- Да бъде централизирана, уеб базирана;
- Да работи с база данни;
- Да поддържа два режима на работа – публичен и непубличен;
- Да позволява многопотребителска работа;
- Да осигури интегритет при управлението на регистрите (използването на единни класификатори/списъци/номенклатури);
- Да осигурява идентификация и автентификация на потребителите при работа с данните (въвеждане, редактиране, заличаване);
- Да позволява динамично управление (създаване, редактиране и заличаване) на роли и привилегии;
- Да позволява динамично управление на потребители (създаване, присвояване/промяна на роли и привилегии, активиране/деактивиране);
- Да поддържа история на данните и на техните промени;
- Да поддържа одитни записи;
- Дизайнът да позволява бъдещо разширение и подобрения, също така и съвместимост със съществуващи външни и вътрешни системи (с цел интегрирането им на следващи фази);
- Публичната част на системата да позволява работа с различни браузъри (Microsoft Internet Explorer, Mozilla, Firefox);
- Системата да извършва проверка на въвежданите от потребителите данни,

като например формат, задължителност и др. Пълният набор проверки следва да се установи по време на етапите анализ и проектиране;

- Системата трябва да осигурява цялостност (интегритет) на данните при многопотребителски режим на работа;
- Системата трябва да осигурява непрекъсната 24/7 работоспособност;
- Да дава възможност са генериране на справки;
- Да има възможност за архивиране и възстановяване както на нейната работоспособност така и на данните.

2. Регистър на длъжностните лица по защита на данните (ДЛЗД)

2.1 Общо описание на регистър ДЛЗД.

Администраторът (АЛД) и обработващият лични данни определят длъжностно лице по защита на данните (ДЛЗД) във всички случаи, когато:

- обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни;
- е налице мащабно обработване на данни по чл. 5 ал. 1 от ЗЗЛД;
- обработването на лични данни е за целите на:
  - отбраната на страната;
  - националната сигурност;
  - опазването на обществения ред и противодействието на престъпността;
  - наказателното производство;
  - изпълнението на наказанията (Доколкото в специален закон не е предвидено друго);
- обработва лични данни на над 10 000 физически лица.

ДЛЗД може да бъде определено и от сдружения, организации или други структури, представляващи категории администратори или обработващи лични данни.

Едно ДЛЗД може да бъде назначено за няколко АЛД/ОЛД/сдружения или организации (по-нататък само АЛД).

АЛД могат да определят повече от едно ДЛЗД.

Администраторът съобщава имената и данните за контакт на ДЛЗД на КЗЛД, както и последващи промени в тях и публикува координатите за връзка с него. Формата и съдържанието на уведомлението и реда за подаването му до Комисията се определят с Правилника за дейността на Комисията и нейната администрация.

ДЛЗД, когато е в мандат, уведомява КЗЛД за промяна на всички обстоятелства свързани с АЛД, залегнали в Уведомлението.

Уведомлението се подава в КЗЛД по един от следните начини:

- По електронен път, при спазване на изискванията на Закона за електронния документ и електронния подпис:
  - Въвеждане/промяна на данните с помощта на екранна форма на САИС;
  - Електронна поща - електронно подписан прикачен файл.
- По пощата - На хартиен носител, в оригинал;
- В приемната на КЗЛД.

2.2 Предназначение на регистър ДЛЗД.

Предназначението на регистъра е да:

- подпомага КЗЛД при изпълнение на надзорните си задължения и правомощия;
- даде възможност на гражданите и на обществеността за контакт с ДЛЗД/АЛД.

Регистърът е електронен и е публичен.

2.3 Описание на данните в регистъра.

2.3.1 **Данни за ДЛЗД**

2.3.1.1 Данни за идентификация на ДЛЗД:

- Име, презиме и фамилия;
- ЕГН/ЛНЧ;
- Идентификационен номер в регистъра.

2.3.1.2 Данни за контакт с ДЛЗД (за конкретен АЛД):

- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

2.3.1.3 Други, допълнителни данни за ДЛЗД (за сега неструктурирани – свободен текст, например: данни за сертификати);

2.3.2 **Данни за АЛД**

2.3.2.1 Данни за идентификация на АЛД:

- Код по БУЛСТАТ/ЕИК;
- Име на АЛД;
- Представляващ/и АЛД - Име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).

- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

2.3.2.2 Други, допълнителни данни за АЛД (за сега неструктурирани – свободен текст).

2.4 Ограничения

- Не всички данни от регистъра са публични;
- Във връзка с чл. 2 от Закона за електронното управление, АЛД/ДЛЗД подават само данни, които са достатъчни за тяхната еднозначна идентификация. КЗЛД получава останалата информация от съответния първичен администратор на данни, по един от следните начини:
  - Автоматично – обмен на заявки между САИС със системи на други организации (например Агенция по вписванията – ТР, РБУЛСТАТ);
  - Автоматизирано – служители на КЗЛД получават необходимата информацията от публични регистри на други организации и я въвеждат в системата.

3. Регистър на акредитирани, сертифициращи организации (АСО)

3.1 Общо описание на регистър АСО

С цел да се демонстрира спазването на Регламент 2016/679 и на Закона при операциите по обработване от страна на администраторите и обработващите лични данни, на същите могат да се издават сертификати.

Организации, притежаващи подходящ опит в областта на защитата на данните могат да издават, подновяват и прекратяват сертификати. Когато тези организации получат акредитация, същите се наричат сертифициращи органи.

Акредитацията на сертифициращи органи се извършва от Комисията за защита на личните данни въз основа на критерии, определени от нея или от Европейския комитет по защита на данните, или от водещия надзорен орган на друга държава членка - при трансгранично обработване на лични данни.

Акредитацията се издава за срок от пет години и може да бъде подновена от Комисията при същите условия.

Комисията за защита на личните данни анулира акредитацията на сертифициращ орган, когато установи, че вече не се спазват условията за акредитация, или че предприетите от сертифициращия орган действия нарушават Закона или Регламент (ЕС) 2016/679.

Критериите, механизмите и процедурите за сертифициране, печати и маркировки се уреждат в наредба, издадена от Комисията за защита на личните данни. Наредбата се обнародва в „Държавен вестник".

След извършване на процедурите по акредитация, сертифициращия орган получава сертификат за акредитация.

Регистърът е електронен и е публичен

3.2 Предназначение на регистър АСО

Предназначението на регистъра е да осигури публичност на сертифициращите органи.

3.3 Описание на данните

3.3.1 Данни за идентификация на сертифициращия орган:

- Идентификационен номер в регистър АСО;
- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование на организацията;
- Представляващ/и организацията - Име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).
- Адрес за кореспонденция:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).
- Адрес на интернет страница.

3.3.2 Данни на лица за контакти:

- Име, презиме и фамилия;
- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

3.3.3 Данни за сертификата:

- Идентификационен номер;
- Дата на издаване на сертификата;
- Дата/Срок на валидност;
- Дата на анулиране на сертификата;
- Описание на причините за анулиране.

3.4 Ограничения

Не всички данни от регистъра са публични. Публичната част на регистъра се урежда с Наредбата по т. 3.1.

4. Регистър на кодекси за поведение (КП)

4.1 Общо описание на регистър КП

Сдруженията и други структури, представляващи категории администратори или обработващи лични данни, могат да изготвят кодекси за поведение или да изменят или допълват такива кодекси с цел да бъде уточнено прилагането на Регламента и закона.

Изготвянето на кодекси за поведение има за цел да допринесат за правилното прилагане на регулаторната рамка, като се отчитат специфичните характеристики на различните АЛД и обработващи данни, по браншове и сектори.

Кодексите за поведение имат наблюдаващи органи. Наблюдаващият орган може да извършва промени в кодексите, за което информира КЗЛД.

КЗЛД одобрява или връща за доработка на проектите на кодексите за поведение. Одобрените кодекси са поведение се вписват в регистъра.

Регистърът е електронен и е публичен

4.2 Предназначение на регистър КП

Регистърът е предназначен да осигури публичност на одобрените кодекси за поведение и техните наблюдаващи органи.

4.3 Описание на данните

4.3.1 Данни за кодексите

- Идентификационен номер в регистър КП;
- Наименование;
- Сектор/бранш;
- Дата на одобрение/публикуване;
- Дата на последна промяна;
- Дата на „заличаване“ в регистъра;
- Описание на обстоятелствата по заличаване.

4.3.2 Данни за издателя на кодекса

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование;
- Представляващ/и - име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).
- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

4.3.3 Данни на лица за контакти:

- Име, презиме и фамилия;

- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

4.3.4 **Данни за органа, акредитиран да наблюдава КП:**

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование;
- Представляващ/и - Име, презиме и фамилия;
- Седалище и адрес на управление (ако е приложимо):
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).
- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

4.4 Ограничения

Не всички данни от регистъра са публични.

5. Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия – Регистър на нарушенията и предприетите мерки (НПМ)

5.1 Общо описание на регистър НПМ

В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо - не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на данните КЗЛД.

Уведомлението се подава в КЗЛД по един от следните начини:

- По електронен път, при спазване на изискванията на Закона за електронния документ и електронния подпис:
  - Въвеждане/промяна на данните с помощта на екранна форма на САИС;
  - Електронна поща - електронно подписан прикачен файл.
- По пощата - На хартиен носител, в оригинал;
- В приемната на КЗЛД.

5.2 Предназначение на регистър НПМ

Предназначението на регистъра е да:

- подпомага КЗЛД при изпълнение на надзорните си задължения и правомощия;
- дава възможност за анализи на причините за възникналите нарушение на

сигурността на данните, с цел идентифициране на тенденции и евентуална превенция.

Регистърът е електронен и НЕ е публичен

5.3 Описание на данните

5.3.1 **Данни за идентификация на АЛД, обект на нарушението:**

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Име на АЛД;
- Представляващ/и АЛД - Име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к .....).

5.3.2 **Данни за нарушението**

- Тип на нарушението (ако е приложимо, да се избира от списък/класификатор на нарушенията);
- Описание на естеството на нарушението на сигурността на данните, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- Описание на евентуалните последици от нарушението на сигурността на личните данни;
- Описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици;
- Дата за събитието/събитията довели до нарушението на сигурността на личните данни (ако е приложимо);
- Дата на уведомяване на КЗЛД;
- Спазен ли е 72-часовия срок (ДА/НЕ);
- Описание на причините за забавянето, когато не е подадено в срок от 72 часа.

5.3.3 **Данни за ДЛЗД или за друго лице за контакт:**

- Име, презиме и фамилия;
- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

5.3.4 Данни за субекта на нарушението – свободен текст

5.3.5 Мерки, предприети от КЗЛД – свободен текст

5.3.6 Ограничения

Информацията може да бъде подадена в КЗЛД, както следва:

- едновременно (цялата);
- поетапно без по-нататъшно ненужно забавяне.