УТВЪРЖДАВАМ:

Дамян Войновски
Заместник изпълнителен директор на
Изпълнителна агенция „Автомобилна администрация“

ПОЛИТИКА
ЗА ЗАЩИТА И ПОВЕРИТЕЛНОСТ НА ЛИЧНИТЕ ДАННИ
В ИЗПЪЛНИТЕЛНА АГЕНЦИЯ „АВТОМОБИЛНА АДМИНИСТРАЦИЯ“

Изпълнителна агенция „Автомобилна администрация“ (агенцията) е създадена през 2002 г. със Закона за автомобилните превози. Агенцията е юридическо лице на бюджетна издръжка към Министерството на транспорта, информационните технологии и съобщенията, със седалище в гр. София и 27 регионални структури.

Дейността, структурата и организацията на агенцията са определени с Устройствен правилник, приет с ПМС № 272 от 29.11.2013 г., обн., ДВ, бр. 105 от 6.12.2013 г., изм. и доп., бр. 33 от 8.05.2015 г., в сила от 15.05.2015 г.

Агенцията се ръководи и представлява от изпълнителен директор, който се назначава от министъра на транспорта, информационните технологии и съобщенията съгласувано с министър-председателя.

Административното ръководство на агенцията се осъществява от главен секретар.

Контролът върху дейността на агенцията се осъществява от министъра на транспорта, информационните технологии и съобщенията.

Структурата на ИА „Автомобилна администрация“ е разпределена в Централно управление и 27 областни отдели.

Адрес на централното управление на Изпълнителна агенция „Автомобилна администрация“: гр. София 1000, ул. "Ген. Й. В. Гурко" № 5, тел: 02/9308840, факс: 02/988 54 95, e-mail: avto_a@rta.government.bg

Длъжностно лице за защита на данните: Стефан Златарев: szlatarev@rta.government.bg

ВЪВЕДЕНИЕ

Считано от 25 май 2018 г. е в сила Регламент (ЕС) 2016/679 (General Data Protection Regulation - GDPR) на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), наричан по-долу „Регламент (ЕС) 2016/679/Регламент/а/ът“.

Регламентът урежда правата и задълженията по защита на личните данни на физическите лица от всички държави членки на Европейския съюз (ЕС).

Агенцията, в качеството си на администратор на лични данни по смисъла на чл. 4, ал. 7 от Регламент (ЕС) 2016/679, осъществява дейността по събиране, обработване и съхранение на лични данни в съответствие с Регламента и Закона за защита на личните данни (ЗЗЛД).

ПРЕДМЕТ И ЦЕЛИ

С тази Политика за защита и поверителност на личните данни (Политиката), Ръководството на агенцията определя правилата по отношение на защитата на физическите лица (служители на агенцията и външни физически и юридически лица) във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни, с което се цели да бъдат защитени основните права и свободи на физическите лица и по-специално тяхното право на защита на личните данни.

Политиката изразява ангажимента на ръководството да изпълнява всички дейности, разглеждайки ги в контекста на защитата на данните и поема отговорно своите задължения и задълженията на своите служители в съответствие с Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

ОБХВАТ

Политиката е разработена в изпълнение на общите изисквания за защита на личните данни на физически или представители на юридически лица. В състава на определението „лични данни" влиза всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"), пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер (ЕГН), данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата,

физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Тази Политика се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

В обхватът на Политиката не се включват дейности, които не са включени в нормативната уредба на Република България и на ЕС или се отнасят до лични или домашни занимания.

Изключение се прави и в случаите на разследване от компетентните органи, свързано с предотвратяването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност. В тези случаи обработването на данните се извършва под контрола на съответния държавен орган.

Настоящата Политика включва обработването на лични данни на субекти на данни, които се намират в ЕС, от администратор или обработващ лични данни, който не е установен в ЕС, когато дейностите по обработване на данни са свързани с предлаганите от агенцията административни услуги и другите предложения в член 3 от Регламента.

ОПРЕДЕЛЕНИЯ НА ИЗПОЛЗВАНИТЕ ИЗРАЗИ

Определенията на „лични данни"; „обработване"; „ограничаване на обработването"; „профилиране"; „псевдонимизация"; „регистър с лични данни"; „администратор"; „обработващ лични данни"; „получател"; „трета страна"; „съгласие на субекта на данните"; „нарушение на сигурността на лични данни"; „генетични данни"; „биометрични данни"; „данни за здравословното състояние"; „основно място на установяване"; „представител"; „дружество"; „група предприятия"; „задължителни фирмени правила"; „надзорен орган"; „засегнат надзорен орган“; „трансгранично обработване“; „относимо и обосновано възражение"; „услуга на информационното общество"; „международна организация" са разписани подробно в член 4 от Регламента.

ПРИНЦИПИ, СВЪРЗАНИ С АДМИНИСТРИРАНЕТО НА ЛИЧНИ ДАННИ

Администрирането на лични данни от оторизираните служители на агенцията се основава на следните основополагащи принципи:

1. **„Законосъобразност, Добросъвестност и Прозрачност**" по отношение на субекта на данните.
2. **„Ограничение на целите"** – събираните данни са за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.
3. **„Свеждане на данните до минимум"** – събират се подходящи данни и ограничени до необходимото във връзка с целите, за които се обработват.
4. **„Точност"** – данните са точни и се поддържат в актуален вид; предприемт се всички нормативно определени мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид и целите, за които те се обработват.
5. **„Ограничение на съхранението"** – данните се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от нормативно определен за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, като се прилагат подходящи технически и организационни мерки, с цел да бъдат гарантирани правата и свободите на субекта на данните.
6. **„Цялостност и поверителност"** – данните се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.
7. **„Отчетност"** - ръководството на агенцията декларира, че събирането и обработването на данни се извършва законосъобразно, добросъвестно и прозрачно и е в състояние да докаже спазването на тези принципи.

Ако конкретната цел или цели, за които се обработват лични данни от агенцията, не изискват или вече не изискват идентифициране на субекта на данните, агенцията не е задължена да поддържа, да се сдобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламента.

ЗАКОНОСЪОБРАЗНОСТ НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Личните данни, които агенцията събира са необходими за спазването на законово задължение за изпълнение на конкретни, точно определени от закона цели, за изпълнението на задачи от обществен интерес, за упражняването на официални правомощия, за изпълнение на договори.

Личните данни събирани за посочените по-горе цели се обработват законосъобразно и добросъвестно и не се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения и/или нормалното функциониране на агенцията.

Събирането, обработването и съхраняването на лични данни в регистрите на агенцията се извършва на хартиен, технически и/или електронен носител, по централизиран и/или разпределен способ, в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Законосъобразността на обработването, видовете данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани лични данни, и целите, за които се разкриват; ограниченията по отношение на целите на разкриването; периодът на съхранение и операциите и процедурите за обработване, включително мерки за гарантиране на законосъобразното и добросъвестно обработване, се определят от законовите и нормативни изисквания към агенцията.

Всеки субект на данни подписва декларация за съгласие по образец (Приложение № 1), като същият има право да оттегли съгласието си по всяко време, когато не са налице целите за събиране, обработване и съхранение на личните данни от агенцията, на физическите лица, а именно:

- за спазването на законово задължение за конкретни, точно определени от закона цели;
- за изпълнението на задачи от обществен интерес;
- за упражняването на официални правомощия;
- за изпълнение на договор.

Право на достъп до регистрите с лични данни имат само оторизираните служители на агенцията, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

Оторизирането на служители се извършва на база длъжностна характеристика или чрез изричен акт на изпълнителният директор на агенцията.

Оторизираните служители и правомощници носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните служители или прекратяване на правомощията на външните организации.

Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения и попълват Декларация за поверителност (*Приложение № 2 и Приложение № 3*)

Документите и преписките, по които работата е приключила, се архивират в изпълнение на Вътрешните правила за дейността на учрежденските архиви в агенцията, утвърдени със Заповед РД-08-13/23.10.2014 г., изм. със Заповед РД-08-6/30.07.2015 г., изм. със Заповед РД-08-7/28.06.2018 г. на изпълнителния директор на агенцията.

Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожароизвестителни системи и пожарогасители, със системи за контрол на достъпа и задължително се заключват .

Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване,

обработващо данните. Достъп до електронните архивите имат само обработващият /операторът/ на лични данни и оторизираните длъжностни лица.

Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица и специализираните държавни органи съобразно възложените им от закона правомощия в присъствието на изпълнителния директор и/или - длъжностното лице за защита на данните.

С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. Проведеният инструктаж се протоколира.

Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от агенцията регистри. Проверките се извършват от комисия, включваща служители на агенцията, които изготвят доклад за резултата от проверката (Доклада/ът), който трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. Докладите се адресират до длъжностното лице по защита на данните и до изпълнителния директор на агенцията.

При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позвалява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му. В интранет страницата на агенцията е приложен и се поддържа регистър на инцидентите (*Приложение № 4*).

При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, Ръководството на агенцията може да

определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на две години или при промяна на характера на обработваните лични данни.

След постигане целта на обработване на личните данни, съдържащи се в поддържаните от агенцията регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящата Политика.

В случаите, в които се налага унищожаване на носител на лични данни се прилагат необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

- личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;
- документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на изпълнителния директор на агенцията и след уведомяване на Длъжностното лице по защита на данните.

За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от упълномощените служители, представляващ утвърден от изпълнителният директор образец.

Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респективно искане за достъп до информация, и след тяхното легитимиране.

Решението си за предоставяне или отказване достъп до лични данни за съответното лице, агенцията съобщава в 1-месечен срок от подаване на заявлението, респективно искането.

Информацията може да бъде предоставена под формата на:

- устна справка;
- писмена справка;

- преглед на данните от самото лице;
- предоставяне на исканата информация на технически и/или електронен носител.

Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец съгласно *Приложение № 5*, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Физическата защита на лични данни в агенцията се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Основните организационни мерки за физическа защита на лични данни в агенцията включват:

1. определяне на помещенията, в които се обработват лични данни.
2. определяне на помещенията, в които се разполагат елементите на комуникационно-информационните системи за обработване на лични данни.
3. определяне на организацията на физическия достъп до тези помещения.

Като помещения, в които се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти

за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

Организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Зони с контролиран достъп са всички помещения на територията на агенцията, в които се събират, обработват и съхраняват лични данни.

Използваните технически средства за физическа защита на личните данни в агенцията са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае" с оглед изпълнението на работните им задължения.

Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Основните технически мерки за физическа защита на лични данни в агенцията включват:

1. Използване на сигнално-охранителна техника;
2. Използване на ключалки и заключващи механизми;
3. Шкафове, метални каси,
4. Оборудване на помещенията с пожароизвестителни и пожарогасителни средства.

Документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

Оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица, заключваеми шкафове и пожарогасителни средства.

Пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Основните мерки за персонална защита на личните данни, приложими в агенцията, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящата Политика, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец.
2. Запознаване и осъзнаване за опасностите за личните данни, обработвани от агенцията.
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.) между персонала и всякакви други лица, които са неоторизирани.
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни (Декларация за конфиденциалност).

За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен посочените мерки и следните допълнителни мерки::

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Основните мерки за документална защита на личните данни, са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на агенцията, сключване на договори, изпълнение на

договори, упражняване на предвидени в закона права и установени от закона задължения.

2. Определяне на условията за обработване на лични данни - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или административна дейност на агенцията, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните.
3. Регламентиране на достъпа до регистрите с лични данни – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";
4. Определяне на срокове за съхранение - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. Процедури за унищожаване: Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на агенцията или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

За лични данни, оценени с по-висока степен на риск, освен посочените мерки, се прилагат и следните допълнителни мерки:

1. Контрол на достъпа до регистрите, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае", за да изпълняват техните задължения.
2. Правила за размножаване и разпространение, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

ПОЛИТИКА ЗА ЗАЩИТАТА НА АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ И/ИЛИ МРЕЖИ

За защита на личните данни, администрирани от агенцията, са включени набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на агенцията. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае";

2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;

3. Управление на външни връзки и/или свързване, включващо от своя страна:

   - Дефиниране на обхвата на вътрешните мрежи:

   Като вътрешни мрежи се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка", които се намират под контрола и администрацията на агенцията. Като външни мрежи се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на агенцията.

   - Регламентиране на достъпа до вътрешната мрежа:

   Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от Изпълнителен директор на агенцията лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае". Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

- Администриране на достъпа до вътрешната мрежа:

Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

- Контрол на достъпа до вътрешната мрежа:

Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на агенцията, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. Защитата от зловреден софтуер включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от Ръководството на агенцията лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на агенцията.

- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Ръководството на агенцията лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

- активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да

уведоми оторизираните от Ръководството на агенцията, лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по създаване и поддържане на резервни копия за възстановяване, която регламентира:

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на агенцията.

- Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

- Отговорност за архивиране имат служителите – системни администратори на агенцията.

- Срокът за съхраняване на архивите е съобразен с действащото законодателство.

- Съхраняването на архива се извършва върху друг сървър, при спазване на всички правила за ограничен достъп в помещението и противопожарна защитаследва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа

6. Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.).

7. Персоналната защита на данните е част от цялостната охрана на агенцията.

8. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на агенцията.

9. Данните, които вече не са необходими за целите на агенцията и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

За лични данни, оценени с по-висока степен на риск, освен горепосочените мерки се прилагат и допълнителни мерки, свързани с:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на агенцията:

   - Отдалечен достъп до вътрешни мрежи на агенцията не е предвиден. По изключение, и след изричната оторизация от Ръководството на агенцията, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

   - На персонала на агенцията може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до елекронните ригистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано с оторизираните от Ръководството на агенцията лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от Ръководството на агенцията. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на агенцията, както и в случаите на заплаха за сигурността на данните.

   - Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Ръководството на агенцията.

2. Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на агенцията, включват:

   - Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на агенцията от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и

способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на агенцията, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

3. Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

По отношение на личните данни се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

Криптирането се използва и за защита на личните данни, които се предават от агенцията по електронен път или на преносими носители.

БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място и след идентификация чрез име и парола към системата. При приключване на работното време служителите заключват локалния си компютър.

Агенцията прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секудни), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

ПРЕДСТАВИТЕЛИ НА АДМИНИСТРАТОРА И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

За изпълнение на основните задачи на агенцията, произтичащи от Закона за автомобилните превози и Закона за движението по пътищата е възложено на външни компании да разработят подходящ и защитен софтуер, с което да се администрират законоустановените дейности, свързани с осъществяване на контрол и регулация на общественият превоз на пътници и товари, издаване на разрешителни за автомобилните превози на опасни товари, проверка на техническата изправност на превозните средства, одобряването на превозни средства, придобиването на правоспособност за управление на моторно превозно средство (МПС), повишаване квалификацията на водачите, психологически подбор и др. дейности определени с национални или европейски нормативни документи. Програмите са инсталирани в офисите на представители на администратора – фирми придобили права и законоустановени разрешителни за работа, които обработват необходимата информация по дейностите на агенцията. Взаимоотношенията между агенцията, софтуерната компания и обработващите лични данни - представители на агенцията, са уредени с договорни взаимоотношения. В тристраннните договори са взети предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, агенцията изисква въвеждане на подходящи технически и организационни

мерки, за да се гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламента и ЗЗЛД. Тези мерки се преразглеждат периодично и при необходимост се актуализират.

Обработващият лични данни и всяко лице, действащо под ръководството на агенцията, което има достъп до личните данни, обработва тези данни само по указание на администратора. Всяко такова лице, оправомощено да обработва личните данни, са подписали декларация за поверителност.

Оправомощените да обработват лични данни организации, подпомагат администратора, чрез подходящи технически и организационни мерки да осигурят сигурност на физическата и електронна среда , в която се обработват лични данни.

Агенцията е публична администрация и в законовото си право е да поддържа регистри за основните си дейности - контрол и регулация на общественият превоз на пътници и товари, издаване на разрешителни за автомобилните превози на опасни товари, проверка на техническата изправност на превозните средства, одобряването на превозни средства, придобиването на правоспособност за управление на МПС, повишаване квалификацията на водачите, психологически подбор и др. нормативно определени.

СЪТРУДНИЧЕСТВО С НАДЗОРНИЯ ОРГАН – КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (КЗЛД)

При поискване администраторът и обработващият лични данни си сътрудничат с надзорния орган при изпълнението на неговите задължения.

Докладването на нарушения и пробиви в сигурността на личните данни, както и уведомяването на КЗЛД се извършва по начин, определен със заповед на изпълнителния директор на агенцията или оправомощено от него лице, при спазване на изискванията на чл. 33 от Регламента, а именно:

1. Докладване до КЗЛД не по-късно от 72 часа след установяване на нарушението на сигурността на личните данни. В доклада се включват следните параметри:

   - описание на естеството на нарушението на сигурността на личните данни, 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 мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

2. Задължение на обработващият лични данни да уведоми и ДЛЗД, без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

3. Агенцията документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на КЗЛД орган да дали са спазени нормативните изисквания.

4. Действия за съобщение до субекта на данни, чиито лични данни са с нарушена сигурност, като се посочват действията и мерките, за ограничаване нарушението на данните.

УПРАВЛЕНИЕ НА РИСКА ПО ОТНОШЕНИЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

В Агенцията са въведени процедури за извършване на оценка на риска на основата на:

- естеството, обхвата, контекста и целите на обработването;
- възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест;
- последиците за правата и свободите на физическите лица.

В процедурата са засегнати:

- Извършването на оценка на въздействието върху защитата на личните данни при наличие на висок риск (напр. в резултат на профилиране, мащабно обработване на специални (чувствителни) лични данни, систематично мащабно наблюдение на публично достъпна зона, нови технологии и др.).

- Задължителна предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.
- Периодичен преглед на избраните технически и организационни мерки, за да може да се гарантира и докаже спазване на Регламента и ЗЗЛД.
- Преглед на мерките за защита на данните на етапа на проектирането и по подразбиране:
  - **на етапа на проектирането**: въвеждане както към момента на определянето на средствата за обработване, така и към момента на самото обработване, на подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване;
  - **по подразбиране**: въвеждане на подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

ПРЕГЛЕД НА ПРОЦЕДУРИТЕ И ОБУЧЕНИЕ

Ръководството на агенцията ще предоставя обучение на всички служители по въпроси, свързани със защитата на данните, по време на въвеждане и редовно след това. Ако служител смята, че желае да се възползва от опреснително обучение, той/тя трябва да се свърже с ДЛЗД г-н Стефан Златарев.

На планирани интервали, агенцията.преглежда спазване на тази политика за да гарантира съответствие с Регламента и ЗЗЛД.

ПОСЛЕДИЦИ ОТ НЕСЪОТВЕТСТВИЕ С РЕГЛАМЕНТА

Неспазването на принципите за защита на данните в рамките на тази политика може да доведе до нарушението на сигурността на личните данни и да породи висок риск за правата и свободите на засегнатите физическите лица. В тези случаи агенцията предприема действия за установяване на виновните служители.Всички служители са задължени да гарантират, че се

съобразяват с принципите за защита на данните при достъпа, използването или унищожаването на лична информация, а именно:

1. „Законосъобразност, Добросъвестност и Прозрачност" по отношение на субекта на данните.

2. „Ограничение на целите" – събираните данни са за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

3. „Свеждане на данните до минимум" - събират се подходящи данни и ограничени до необходимото във връзка с целите, за които се обработват.

4. „Точност" – данните са точни и се поддържат в актуален вид; предприемт се всички нормативно определени мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид и целите, за които те се обработват.

5. „Ограничение на съхранението" – данните се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от нормативно определен за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, като се прилагат подходящи технически и организационни мерки, с цел да бъдат гарантирани правата и свободите на субекта на данните.

6. „Цялостност и поверителност" – данните се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

7. „Отчетност" - Ръководството на Изпълнителна агенция „Автомобилна администрация“.. декларира, че събирането и обработването на данни се извършва Законосъобразно, Добросъвестно и Прозрачно и е в състояние да докаже спазването на тези принципи.

Приложение № 1

към Политиката за поверителност на данните

ДЕКЛАРАЦИЯ

Долуподписаният/ната

.....

(име, презиме и фамилия на лицето)

ЕГН: .....

ДЕКЛАРИРАМ:

Съгласен/на съм Изпълнителна агенция „Автомобилна администрация“ да обработва и съхранява личните ми данни, които предоставям във връзка с .....

.....

.....

Запознат/а съм с Процедурата за защита на личните данни, както и с:

- целта и средствата на обработка на личните ми данни;
- доброволния характер на предоставянето на данните;
- правото на достъп и на коригиране на събраните данни.

С настоящата декларация декларирам съгласие за обработка и съхранение на личните ми данни при спазване на разпоредбите на Закона за защита на личните данни и РЕГЛАМЕНТ

(ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/БО (Общ регламент относно защитата на данните).

дата .....

гр. ..... ДЕКЛАРАТОР: .....

Приложение № 2

(за служители на Изпълнителна агенция „Автомобилна администрация")

ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ

От.....,

(име, презиме, фамилия)

ЕГН .....,

Длъжност:.....,

Дирекция: .....,

Отдел: .....

В качеството си на служител на Изпълнителна агенция „Автомобилна администрация".. имащ служебен достъп до лични данни, за минималното ниво на технически и организационни мерки и допустимия вид за защита на личните данни

ДЕКЛАРИРАМ:

ЗАПОЗНАТ съм:

1. С нормативната уредба в областта на защитата на личните данни - РЕГЛАМЕНТ 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, ЗЗЛД и издадените въз основа на тях нормативни

документи, включително и Вътрешни правила за технически и организационни мерки и допустимия вид за защита на личните данни в Изпълнителна агенция „Автомобилна администрация“...

2. С политиката и ръководствата за защита на личните данни в Изпълнителна агенция „Автомобилна администрация“...

3. С опасностите за личните данни, обработвани Изпълнителна агенция „Автомобилна администрация“.. в качеството си на администратор на лични данни.

4. Няма да споделям критична информация с трети лица, включително и с лица от персонала като например: идентификатори, пароли за достъп и т.н.;

5. Съгласен съм и поемам задължение за неразпространение на личните данни, до които съм получил достъп при и по повод изпълнение на задълженията си Изпълнителна агенция „Автомобилна администрация“.

..... 07. 2018 г. .....

(декларатор - подпис)

Приложение № 3

(за оправомощени от Изпълнителна агенция „Автомобилна администрация“ лица)

ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ

От.....,

(име, презиме, фамилия)

ЕГН .....

Длъжност: .....

Служител на: .....

Организация: .....

В качеството си на служител на ....., която е правомощник на

(име на организацията)

Изпълнителна агенция „Автомобилна администрация“.. и имаща служебен достъп до лични данни, за минималното ниво на технически и организационни мерки и допустимия вид за защита на личните данни

ДЕКЛАРИРАМ:

ЗАПОЗНАТ съм:

1. С нормативната уредба в областта на защитата на личните данни - РЕГЛАМЕНТ 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, ЗЗЛД и издадените въз основа на тях нормативни документи, включително и Вътрешни правила за технически и организационни мерки и допустимия вид за защита на личните данни в Изпълнителна агенция „Автомобилна администрация“.
2. С политиката и ръководствата за защита на личните данни в Изпълнителна агенция „Автомобилна администрация“.
3. С опасностите за личните данни, обработвани Изпълнителна агенция „Автомобилна администрация“.. в качеството си на администратор на лични данни.
4. Няма да споделям критична информация с трети лица, включително и с лица от персонала като например: идентификатори, пароли за достъп и т.н.;
6. Съгласен съм и поемам задължение за неразпространение на личните данни, до които съм получил достъп при и по повод изпълнение на задълженията си Изпълнителна агенция „Автомобилна администрация“.

..... 07. 2018 г. .....

(декларатор - подпис)

Приложение № 4

Регистър за докладване и управление на инциденти свързани с неправомерен достъп до информационните масиви за лични данни

рег. №						
дата						

Кой е установил нарушението						
час на установяване						
Какво е нарушението						
какви лични данни са засегнати						
брой на засегнатите субекти на лични данни						
брой на засегнати записи						
на кого е докладвано						
дата						
час на докладването						
какви мерки са предприети за ограничаване на въздействието от нарушението						
кога е докладвано на ДЛЗД						

дата						
час						
кога е докладвано на КЗЛД						
дата						
час						

Приложение № 5

СПОРАЗУМЕНИЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Днес, ... г., между страните:

Изпълнителна агенция „Автомобилна администрация“, Булстат 121410441, с адрес в гр. София 1000, ул. “Ген. Й. В. Гурко” № 5, представлявана от ..... – ....., наричано по-нататък “Администратор” и

....., ЕИК: ....., с адрес ....., представлявано от ..... – ....., наричано по-нататък “Обработващ”, на основание на член 28 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), се сключи настоящото споразумение, което е неразделна част от договора между страните, сключен на ..... (Договора).

I. ПРЕДМЕТ

1. Във връзка с Договора, Администраторът възлага, а Обработващият се задължава да обработва лични данни от името и за сметка на Администратора в съответствие с целта и условията, определени в настоящото споразумение и Закона за защита на личните данни и Общия регламент относно защитата на данните.

II. ОПРЕДЕЛЕНИЯ

2. „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко

или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

2.1. „Администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държава членка.

2.2. „Обработващ“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

2.3. „Обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

III. СРОК НА ДЕЙСТВИЕ НА ОБРАБОТВАНЕТО

3. Срокът на действие на обработването на личните данни е от момента на предаването им от страна на Администратора до прекратяване на Договора по реда и сроковете, предвидени в него.

IV. ЦЕЛ НА ОБРАБОТВАНЕТО

4. Целта на обработването на личните данни са изпълнението на услугите по предмета на Договора.

V. ВИДОВЕ ЛИЧНИ ДАННИ

5. Видовете лични данни, които могат да бъдат обработвани, са свързани с основните задачи на агенцията, произтичащи от Закона за автомобилните превози и Закона за движението по пътищата, свързани с осъществяване на контрол на техническата изправност на превозните средства, придобиването на правоспособност за управление на МПС, повишаване квалификацията на водачите, психологически подбор и др. дейности определени с национални или европейски нормативни документи.

VI. КАТЕГОРИИ СУБЕКТИ НА ДАННИ

6. Категориите субекти на данни могат да бъдат клиенти и контрагенти на Администратора.

VII. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ

7. Обработващият се задължава:

а) да обработва личните данни само по документирано нареждане на Администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на ЕС или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира Администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес. С оглед избягване на всякакво съмнение, за документирано нареждане се смята и изпращането или предаването на документи, данни и информация за изпълнението на услугите по Договора, както и на допълнителни услуги, възложени от Администратора на Обработващия.

б) да гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност;

в) да вземе всички необходими мерки съгласно член 32 от Общия регламент относно защитата на данните;

г) ако включва друг обработващ лични данни, като подизпълнител за извършването на специфични дейности по обработване от името на Администратора, на това друго лице се налагат същите задължения за защита на данните, така че обработването да отговаря на изискванията на Общия регламент за защита на личните данни. Когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този друг обработващ лични данни. Обработващият данни не включва друг обработващ данни, като подизпълнител без предварителното конкретно или общо писмено разрешение на Администратора. В случай на общо писмено разрешение, обработващият данни винаги информира администратора за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като по този начин даде възможност на администратора да оспори тези промени.

д) като вземе предвид естеството на обработването, да подпомага Администратора, доколкото е възможно, чрез подходящи технически и

организационни мерки при изпълнението на задължението на Администратора да отговори на искания за упражняване на предвидените в глава III от Общия регламент относно защитата на данните права на субектите на данни.

е) да подпомага Администратора да гарантира изпълнението на задълженията съгласно членове 32—36 от Общия регламент относно защитата на данните, като отчита естеството на обработване и информацията, до която е осигурен достъп на Обработващия лични данни.

ж) да заличава всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на ЕС или правото на Република България не изисква тяхното съхранение. С оглед защита на своите легитимни интереси Обработващият има право да запази определени данни и информация и след този срок до изтичане на давностния срок за извършване на проверка от Администратора.

з) да осигурява достъп на Администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява извършването на одити, включително проверки, от страна на Администратора или друг одитор, оправомощен от Администратора.

7.1. Обработващият уведомява Администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни. В уведомлението се съдържа най-малко следното:

а) описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) 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.

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

7.2. Администраторът се задължава:

а) да уведоми субекта на данните за предаването на личните му данни на Обработващия;

б) да не предава лични данни на Обработващия, които не са необходими за извършване на услугите по предмета на Договора или допълнително възложени услуги от Администратора;

в) да подава данни, информация и документи към Обработващия само по ред, начин и срокове, определени от Обработващия;

г) да подава на Обработващия само лични данни, които са необходими за извършване на услугите по предмета на Договора.

7.3. Обработващият се задължава да не разкрива лични данни, предоставени от Администратора на трети лица, освен в случаите когато:

а) това е необходимо за изпълнение на услугите по предмета на Договора;

б) това е необходимо за изпълнение на нормативно установено задължение на Обработващия;

в) информацията е изискана от държавни органи или длъжностни лица, които според действащото законодателство са оправомощени да изискват и събират такава информация при спазване на законово установените процедури;

г) други законни основания.

VIII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

8. С подписването на настоящото споразумение Обработващият гарантира, че прилага подходящи технически и организационни мерки по такъв начин, че обработването протича в съответствие с изискванията на Общия регламент относно защитата на данните и осигурява защита на правата на субектите на данни.

8.1. Техническите и организационните мерките за защита на личните данни, които Обработващия прилага включват, без да се ограничават до:

а) Криптиране на лични данни;

б) Премахване на достъп до USB и други преносими носители с памет от работните компютри, използвани за договорената дейност;

в) Ограничаване на достъпа до Интернет от работните компютри, използвани за договорената дейност, като достъпът е разрешен само до определени сайтове на български институции и други сайтове, строго необходими за извършване на дейността на Обработващия;

г) Използване само на проверен и предварително одобрен лицензиран софтуер (регламентиран софтуер) и използване на антивирусен софтуер, защитни стени и proxy сървър;

д) Ограничителни мерки, възпиращи инсталирането и използването на нерегламентиран софтуер, приложения, социални мрежи, месинджъри и др. подобни на работните компютри, използвани за договорената дейност;

е) Защита с парола и персонални права за достъп до базите и директориите с клиентска информация;

ж) Автоматично заключване на бездействащи работни компютри в мрежата;

з) Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;

и) Контрол на физическия достъп до електронни и хартиено базирани записи;

й) Оборудване със сигнално охранителна техника;

к) Прилагане на адекватни вътрешни правила и обучения на персонала във връзка с обработване, съхранение и сигурността на личните данни и поверителната информация;

л) Редовна проверка и контрол на ефективността на своите предпазни мерки, контролни механизми, системи и процедури, включително провеждане на сканиране на уязвимости и корекция на откритите уязвимости.

IX. ОБЩИ РАЗПОРЕДБИ

9. Настоящото споразумение може да бъде изменяно и/или допълвано само със съгласието на страните, изразено в писмена форма от оторизираните представляващи на двете страни.

9.1. За всеки спор относно съществуването и действието на настоящото или във връзка с неговото нарушаване, включително спорове и разногласия относно действителността, тълкуването, прекратяването, изпълнението или неизпълнението му, се прилага българското гражданско и търговско законодателство, като страните уреждат отношенията си чрез споразумение. При непостигане на съгласие, спорът се отнася до компетентния съд.

9.2. С подписване на настоящото споразумение всяка страна декларира, че предоставя доброволно включените лични данни в него, а другата страна поема задължение да обработва предоставените данни съгласно изискванията на закона.

9.3. Ако някоя от разпоредбите на настоящото споразумение се окаже недействителна, неизпълнима или не е в сила поради изменение на Закона или по друг начин, то това няма да повлияе върху действителността или тълкуването на която и да е друга част от условията на

споразумението или Договора, доколкото е възможно всички останали клаузи остават в сила и са задължителни за страните по него.

Настоящото споразумение се подписа в два еднообразни екземпляра – по един за всяка от страните.

За администратора: . . . . . За обработващия: . . . . . .

Съгласувано с: Мариана Китова
И.д. главен секретар

Бисерка Кунарова
Директор на дирекция АПО

31.07.2018

Изготвил: Стефан Златарев
Длъжностно лице по защита на данните