УТВЪРДИЛ: Петя Игнатова Тодорова
УПРАВИТЕЛ НА „Грийн такси“ ООД с ЕИК 201765343

ИНСТРУКЦИЯ №1

за мерките за защитата във връзка с обработването на лични данни и относно свободното движение на такива данни, обработвани във „Грийн такси“ ООД с ЕИК 201765343

Общи положения

Чл. 1. (1) Настоящата Инструкция се издава на основание 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), както и на основание Закона за защита на личните данни (ЗЗЛД) и Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и се прилага от 25.05.2018г.

(2) Инструкцията урежда обработването, съхранението и мерките за защита на личните данни, условията и реда за водене на регистри, както и организацията и реда за упражняване на контрол при обработването на лични данни във „Грийн такси“ ООД с ЕИК 201765343, съгласно Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 /наричано по- долу за краткост Регламента/ и ЗЗЛД.

(3) „Обработване“ на лични данни означава всяка операция или съвкупност от операции, извършвана от „Грийн такси“ ООД с ЕИК 201765343 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;

(4) „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;

(5) Настоящата инструкция не се прилага по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран. Ето защо настоящата инструкция не се отнася за обработването на такава анонимна информация, включително за статистически или изследователски цели.

Чл. 2. (1) Инструкцията се приема с цел да регламентира:

1.Създаването на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на физическите лица, при неправомерно обработване на свързаните с тях лични данни, в процеса на свободно движение на данните.

2.Видовете регистри, които се водят във „Грийн такси“ ООД с ЕИК 201765343.

3.Оценката на въздействието и нивото на защита за всеки от водените регистри с лични данни.

4.Необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване. Мерките имат за цел да гарантират поверителност, цялостност и наличност на личните данни.

5.Правата и задълженията на длъжностните лица, обработващи лични данни и лицата, които имат достъп до лични данни, както и тяхната отговорност при изпълнението на тези задължения.

6.Правила за предоставяне на лични данни на трети лица.

7. Права на субектите на данни и процедури по упражняване на правата на субектите на данни- право на информация, право на достъп до данни, право на изтриване на данни, право на ограничаване на обработването на данни, право на преносимост на данни и право на възражение.

8. Срокове за съхранение на личните данни и реда за тяхното унищожаване след изтичането им.

(2) Инструкцията се утвърждава, допълва, изменя и отменя от един от управителите на „Грийн такси“ ООД с ЕИК 201765343.

II. Администратор, обработващ лични данни и регистри с лични данни

Чл.3. Администратор на лични данни е „Грийн такси“ ООД с ЕИК 201765343, със седалище и адрес на управление: гр. София, Район „Студентски“, „Арсо Пандурски“, кв. 9, срещу РУМ

Чл.4. (1) Обработващ личните данни е всяко физическо или юридическо лице, което обработва лични данни от името на администратора на лични данни.

(2) Отношенията между администратора и обработващия лични данни се уреждат с писмен акт на администратора, в който се определя обемът на правата и задълженията във връзка с обработването на лични данни.

(3)Администраторът може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита.

(4) Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае" и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни на основание чл.7, ал.5 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, до които са получили достъп при и по повод изпълнение на задълженията си.

(5)Всички лица по ал.1, отговарят за спазването на ограниченията за достъп до личните данни, и са персонално отговорни пред Управителя на „Грийн такси“ ООД с ЕИК 201765343 за нарушаването на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства.

Чл. 5. Във „Грийн такси“ ООД с ЕИК 201765343 се обработват лични данни в следните регистри:

1.Регистър „Персонал".

2.Регистър „Услуги“.

I. Регистър „Персонал".

Чл. 6. Описание на поддържания регистър

В регистъра се обработват лични данни на служители, работещи във „Грийн такси“ ООД с ЕИК 201765343 по трудови правоотношения и граждански договори с цел:

1.индивидуализиране на правоотношения по трудови договори по Кодекса на труда и по граждански договори ;

2.изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството и подзаконовите нормативни актове за прилагането им, ЗДДФЛ, Закона за държавния архив.

3.използване на събраните данни за съответните лица за служебни цели:

-за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите правоотношения;

-за изготвяне на всякакви документи на лицата в тази връзка (договори, заповеди, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

-за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови договори и гражданскоправни договори;

-за водене на счетоводна отчетност, относно възнагражденията на посочените по-горе лица по трудови правоотношения и правоотношенията по граждански договори.

Чл.7. (1) Категории лични данни в регистъра и основание за обработването им .

Обработването на лични данни, съдържащи се в регистър „Персонал“ се извършва на някое от следните законови основания:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели:

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

(2) В регистъра се обработват следните категории лични данни:-

1.имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефони за връзка и др.) – обработват се на което и да е от основанията по чл.7;

2.данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография - обработват се на което и да е от основанията по чл.7;

3.номера на банкови сметки на служителите и месечните доходи.

4. данни относно семейното положение на физическото лице (наличие на брой членове на семейството, в това число деца до 18 години; наличие на обстоятелствата по чл. 144 от Семейния кодекс - обработват се на което и да е от основанията по чл.7;

5.гражданско-правен статус на лицата, напр. свидетелства за съдимост –обработват се на което и да е от основанията по чл.7;

6.лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство за започване на работа, експертни лекарски решения, болнични листове и др.– обработват се на което и да е от основанията по чл.7;

(3) Личните данни по чл. 7, ал.2 т.6, които се отнасят до здравето, се обработват както на посочените в ал.2 т.6 основания, така и ако е налице някое от следните условия:

а) субектът на данните е дал съгласие за обработване на личните му данни;

б) обработването е необходимо за изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила;

в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

д) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

е) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на европейското или национално законодателство или съгласно договор с медицинско лице;

ж) обработването е необходимо за целите на архивирането в обществен интерес.

(4) Право на достъп до данните в регистър „Персонал” имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане изразено писмено;

2. Управителите - при изпълнение на законовите им правомощия.

3. Главният счетоводител и/или длъжностни лица, осъществяващ технически операции по обработката и контрол на данните.

4. Дружества обработващ лични данни - Счетоводни компании – юридически лица, с които „Грийн такси“ ООД има сключен договор за счетоводно обслужване.

5. Държавни органи, надлежно легитимирали се със съответни документи, при наличие на законово основание за достъп до данните.

Чл. 8. Описание на регистъра

1. Носители на данни

Данните в регистъра се обработват на хартиен и електронен носител. Автоматизираната обработка на данните във **„Грийн такси“ ООД** с ЕИК 201765343 се осъществява посредством операционни системи и лицензирани софтуерни продукти, в комбинация със специализиран софтуер за обслужване на предмета на дейност.

2.Начин на обработване

Данните в регистъра се предоставят от физическите лица при назначаване във **„Грийн такси“ ООД** с ЕИК 201765343 или след сключване на трудовия или гражданскоправен договор, при упражняване на техни законови права и изпълнение на законни задължения, във връзка с трудовоправното или гражданскоправното им правоотношение. Данните се въвеждат в договори на служителите, споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др, съдържащи се в трудови досиета /папки/ на служителите и гражданскоправните договори, както и в специализирани софтуерни програми и платформи за обработване на данните.

3.Срок за съхранение

Данните в регистъра се съхраняват за срок от 50 години след напускане или пенсиониране, във връзка с нормативно установени срокове;

Чл. 9. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения.

1.Данните от регистъра се обработват от Главния счетоводител и/или длъжностни лица, в чиято длъжностна характеристики е вменено задължение за обработване на данните на служителите, както и от Дружества обработващ лични данни - Счетоводни компании – юридически лица, с които „Грийн такси“ ООД има сключен договор за счетоводно обслужване.

2.Право на достъп до регистъра имат само оправомощените лица.

Чл.10. Оценка на въздействието и определяне съответното ниво на защита на регистъра „Персонал“.

(1) За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица се взима в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност", „цялостност" и „наличност". Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

(2) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. Това се изпълнява след съставянето и оповестяването на списък от Надзорният орган /Комисията за защита на личните данни/ на видовете операции по обработване, за които се изисква оценка на въздействието, но само в случай, че част от дейностите по обработване, извършвани от Администратора, попаднат в позитивния списък /с видовете операции по обработване, за които се изисква извършване на такава оценка/.

(3) В зависимост от определеното средно ниво на въздействие нивото на защита на регистър „Персонал" е средно:

1.имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефони за връзка и др.) –

Ниво на въздействие: поверителност- **средно** цялостност **средно** наличност- **средно**

2.данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография

Ниво на въздействие : поверителност- **ниско** цялостност **ниско** наличност- **ниско**

3.номера на банкови сметки на служителите и месечните доходи

Ниво на въздействие: поверителност- **средно** цялостност **средно** наличност- **средно**

4. данни относно семейното положение на физическото лице (наличие на брой членове на семейството, в това число деца до 18 години; наличие на обстоятелствата по чл. 144 от Семейния кодекс

Ниво на въздействие: поверителност- **ниско** цялостност **ниско** наличност- **ниско**

5.гражданско-правен статус на лицата, напр. свидетелства за съдимост –обработват се на което и да е от основанията по чл.7

Ниво на въздействие: поверителност- **средно** цялостност **средно** наличност- **средно**

6.лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство за започване на работа, експертни лекарски решения, болнични листове и др.–

Ниво на въздействие: поверителност- **средно** цялостност **средно** наличност- **средно**

Чл. 11. (1) Администраторът прилага Технически и организационни мерки за защита.

(2). При обработването на лични данни ръчно и автоматизирано с цел гарантиране на подходящо ниво на сигурност, включително поверителност, Администраторът гарантира сигурността на данните, чрез прилагане на специализирани мерки за защита:

1. „Псевдонимизация“ - за данните на хартиен носител /обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки/. Документите се съхраняват в папки с номера. Списъците, съдържащи идентификационните номера на папките и съответстващите им категории данни и съдържание на папките, отговарящо на номера, се съхраняват отделно и са на разположение само на оправомощени служители.

„Криптиране“ – за данните на електронен носител /кодиране на информацията по начин, който предотвратява достъпа на неоторизирани лица до нея/, чрез използване на комуникационен канал SSL/TLS на email сървъра при електронен обмен на лични данни с трети страни, както и лични пароли за достъп до компютрите на всяко едно от лицата, чийто служебни задължения включват обработване на лични данни от регистъра.

(3) Извън случаите на прехвърляне на данни към държавни институции (НАП, НОИ и др.) с оглед изпълнение на нормативните задължения, както и на данни, които се предоставят на кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служителите, в случаите на предоставяне на достъп до лични данни на трети лица, включително по силата на договори с външни лица (фирми за правни, счетоводни, IT услуги), информацията се предоставя на съответните получатели посредством криптирани канали (при електронно прехвърляне) или при задължително подписване на декларация за конфиденциалност (при предаване на документи на хартиен носител).

Чл. 12. Видове мерки за защита

1. Физическа защита

Всички документи на хартиен носител, съдържащи лични данни, са с ограничен достъп само за упълномощени лица.

Физически достъп до помещенията, в които се обработват лични данни от регистъра се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители.

2.Персонална защита

Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в трудовото досие на всеки обработващ лични данни.

Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

3.Документална защита

Регистър „Персонал" се поддържа на хартиен носител. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в шкаф при Главния счетоводител или оправомощено длъжностно лице. Достъпът до регистъра е ограничен само за упълномощени лица.

Документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават, чрез нарязване на специално устройство (шредер), след изтичане на срока за съхранение, за което се съставя протокол от Главния счетоводител.

4.Защита на автоматизирани информационни системи и мрежи.

- При работа с данните от регистъра се използва софтуерен продукт за обработване. Данните се въвеждат в база данни и се съхраняват на работния компютър където се обработват личните данни. Упълномощените да обработват лични данни лица имат личен профил (потребителско име и парола). Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

След изтичане на срока за съхранение, личните данни на електронен носител се изтриват /заличават/, чрез заличаването им в съответния софтуерен продукт и в базата данни на работния компютър на упълномощения служител /упълномощените служители/.

- В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията.

Чл. 14. Предоставяне на лични данни на трети лица.

(1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

(2)В качеството си на работодател, **„Грийн такси“ ООД** с ЕИК 201765343 може да предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения или обещетения на служители, както и по молба от работещите в дружеството, във връзка с отпускането на кредити на служителите. Личните данни, които се предоставят са три имена и единен граждански номер, постоянен адрес и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането, както и размер на трудовото възнаграждение на лицето за определен период от време, в полза на което се извършва кредитирането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови операции.

(3)В качеството си на работодател, **„Грийн такси“ ООД** с ЕИК 201765343 може да предоставя лични данни и на Дружества обработващ лични данни - Счетоводни компании – юридически лица, с които „Грийн такси“ ООД има сключен договор за счетоводно обслужване.

II. Регистър „Услуги “

Чл. 15. (1) Описание на поддържания регистър.

В регистъра се обработват лични данни на лица, набирани във връзка с извършването на основната дейност на Администратора предоставяне на таксиметрови услуги, както и във връзка с административно – правното и счетоводно обслужване на дружеството и техническата поддръжка на материалната му база и др.

(2) Обработването на лични данни, съдържащи се в регистър „Услуги“ се извършва на някое от следните законови основания.

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора.

(3) Данните в регистър „Услуги“ се обработват с оглед: индивидуализиране на субекти-страни по сключвани договори; използване на събраните данни в изпълнение на нормативни изисквания, свързани с осъществяване на основната дейност на Администратора; в изпълнение на нормативни изисквания за набиране и съхранение на определени документи при осъществяване на основната дейност на Администратора; за установяване на контакт с лицата по телефон, по електронен път за изпращане на кореспонденция, отнасяща се до упражняване на права или изпълнение на задълженията им по сключени договори или поети ангажименти;

Чл. 16. Категории лични данни в регистъра и основание за обработването им

(1) В изпълнение на принципа за законосъобразност и минимизиране на данните в регистъра се обработват следните категории лични данни:

- имена, ЕГН, постоянен, настоящ и електронен адрес и др.- обработват се на което и да е от основанията по чл.15.

(2) Право на достъп до данните в регистър „Услуги” имат:

1. Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане изразено писмено;

2. Управителят - при изпълнение на законовите му правомощия.

3. Главният Счетоводител на „Грийн такси“ ООД с ЕИК 201765343, служители на дружеството, в чиито длъжностна характеристика е определено задължение за обработване на данните на външни лица и при спазване на принципа „Необходимост да се знае".

4. Държавни органи, надлежно легитимирали се със съответни документи, при наличие на законово основание за достъп до данните.

Чл. 17. Описание на регистъра

1.Носители на данни

Данните в регистъра се обработват на хартиен и електронен ~~н~~осител.

2.Начин на обработване

Данните в регистъра се предоставят от съответните лица, с оглед: изпълнение на нормативно регламентирани задължения във връзка със сключване на търговски договори с Администратора:

3. Срок за съхранение на информацията: Данните в регистъра се съхраняват за следните срокове, съобразно номенклатурата на делата за архивиране:

- търговски договори - 10 години след приключване на договора;

- служебни бележки и удостоверения за изплатени възнаграждения -10 г. след одитиране /финансова ревизия.

-фактури и други счетоводни документи – според законово определените минимални срокове.

- регистрационни данни на клиенти, събирани по електронен път с оглед осигуряване на възможност за онлайн поръчки за ползване на таксиметрова услуга – до получаване на искане на субекта за заличаване на данните му, когато е приложимо.

(2) Сроковете по ал. 1 подлежат на изменение, в съответствие с актуалната нормативната уредба във връзка с архивирането на документи и законовите срокове за съхранение на документи от Администратора.

Чл.18. Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

1. Данните от регистъра се обработват от Главния счетоводител на „Грийн такси“ ООД с ЕИК 201765343, служители на дружеството, в чиито длъжностна характеристика е определено задължение за обработване на данните на външни лица и при спазване на принципа „Необходимост да се знае".

2.Право на достъп до регистъра имат само оправомощените лица.

3.Длъжностните лица нямат право да разпространява информация за личните данни, станали им известни при изпълнение на служебните му задължения.

Чл.19. Оценка на въздействието и определяне съответното ниво на защита на регистъра „Услуги“.

(1) За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица се взима в предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност", „цялостност" и „наличност". Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

(2) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. Това се изпълнява след съставянето и оповестяването на списък от Надзорният орган /Комисията за защита на личните данни/ на видовете операции по обработване, за които се изисква оценка на въздействието, но само в случай, че част от дейностите по обработване, извършвани от Администратора, попаднат списъка с видовете операции по обработване, за които се изисква извършване на такава оценка)

(3).В зависимост от определеното средно ниво на въздействие нивото на защита на регистър „Услуги" е средно:

имена, ЕГН, постоянен и настоящ адрес и др.
Ниво на въздействие: поверителност- **средно** цялостност **средно** наличност- **средно**

Чл.20. (1) Администраторът прилага Технически и организационни мерки за защита.

(2). При обработването на лични данни ръчно и автоматизирано с цел гарантиране на подходящо ниво на сигурност, включително поверителност, Администраторът гарантира сигурността на данните, чрез прилагане на специализирани мерки за защита:

1. „Псевдонимизация" - за данните на хартиен носител /обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки/. Документите се съхраняват в папки с номера. Списъците, съдържащи идентификационните номера на папките и съответстващите им категории данни и съдържание на папките, отговарящо на номера, се съхраняват отделно и са на разположение само на оправомощени служители.

2. „Криптиране" – за данните на електронен носител /кодиране на информацията по начин, който предотвратява достъпа на неоторизирани лица до нея/, чрез използване на комуникационен канал SSL/TLS на email сървъра при електронен обмен на лични данни с трети страни.

3. „Криптиране" – за данните на електронен носител /кодиране на информацията по начин, който предотвратява достъпа на неоторизирани лица до нея/ получавани онлайн от клиенти на таксиметрова услуга.

4. (3) Извън случаите на прехвърляне на данни към държавни институции (НАП, НОИ и др.) с оглед изпълнение на нормативните задължения, както и на данни, които се предоставят на кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служителите, в случаите на предоставяне на достъп до лични данни на трети лица, включително по силата на договори с външни лица (фирми за правни, счетоводни, IT услуги), информацията се предоставя на съответните получатели посредством криптирани канали (при електронно прехвърляне) или при задължително подписване на декларация за конфиденциалност (при предаване на документи на хартиен носител).

Чл.21 Видове мерки за защита

1. Физическа защита

Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения при Глания счетоводител и/или при лицата, оправомощени по чл.18. Помещенията,

в които се обработват и съхраняват лични данни от регистъра са защитени от посегателства чрез заключване на вратата. Физически достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

Външни лица имат достъп до помещенията, в които се обработват лични данни от регистъра, само в присъствието на упълномощени служители.

2.Персонална защита

Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в трудовото досие на всеки служител.

Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

3.Документална защита

Регистър „Услуги" се поддържа на хартиен носител. Данните се класифицират в съответствие с тяхното предназначение и характер.

Документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават, чрез нарязване на специално устройство (шредер), след изтичане на срока за съхранение, за което се съставя протокол от главния счетоводител.

4.Защита на автоматизирани информационни системи и мрежи.

- При работа с данните от регистъра се използват софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на работния компютър където се обработват личните данни. Упълномощеният служител/ упълномощените служители има/имат личен профил (потребителско име и парола). Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

- Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система и мрежови устройства. Ежедневно информацията се архивира и се съхранява на твърдия диск.

- След изтичане на срока за съхранение, личните данни на електронен носител се изтриват /заличават/, чрез заличаването им в съответния софтуерен продукт и в базата данни на работния компютър на упълномощения служител /упълномощените служители/.- Администраторът осигурява заличаване по такъв начин, че да е невъзможно тяхното възстановяване, а при наличие на софтуерна възможност осигурява автоматично заличаване на данни, когато обработването им е скрепено със срок.

- В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията и сигнално-охранителна система

Чл. 22. Предоставяне на лични данни на трети лица

Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.)р както и на Дружества обработващ лични данни - Счетоводни компании – юридически лица, с които „Грийн такси" ООД има сключен договор за счетоводно обслужване.

III. Права на субектите на лични данни

Право на информация

Чл.23 (1)Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да получи в кратка, разбираема и лесно достъпна форма, на ясен и прост език, писмено или по друг подходящ начин, включително чрез електронни средства, информация относно:

1. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

2. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

3. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

4. когато обработването се извършва за целите на легитимните интереси на администратора или на трета страна, законните интереси, преследвани от администратора или от трета страна;

5. получателите или категориите получатели на личните данни, ако има такива;

6. съответните категории лични данни- приложимо само когато личните данни не са получени от субекта на данните,

7. когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация;

8. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

9. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;

10. когато обработването се основава на дадено съгласие, съществуването на право на оттегляне на съгласието;

11. правото на жалба до надзорен орган;

12. дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени – **приложимо само за когато личните данни са получени от субекта на данните.**

13.съществуването на автоматизирано вземане на решения, включително профилирането и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

14. Когато администраторът възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел - п**риложимо само когато личните данни са получени от субекта на данните.**

15. източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник- п**риложимо само когато личните данни не са получени от субекта на данните.**

(2) Информацията по ал.1 може да бъде предоставяна и чрез публикуването й в кратък, обобщен и разбираем вид чрез препращащ линк/ под формата на линк, присъстващ в електронната кореспонденция на „Грийн такси“ ООД с ЕИК 201765343, както и на интернет сайта на дружеството и други софтуерни продукти използвани от последното.

(3). В случаите, в които администраторът получава личните данни пряко от субектите, за които се отнасят, задължението за информиране следва да бъде изпълнено в момента на получаване на данните.

(4) В случаите, в които администраторът не получава личните данни пряко от субектите, за които се отнасят, задължението за информиране следва да бъде изпълнено:

- в срок най-късно до месец от получаване на данните ;

- ако данните се използват във връзка със самия субект, най-късно при осъществяване на първия контакт с него;

- ако данните се разкриват пред друг получател, най-късно при първото им разкриване пред него.

(5) Алинея 1 не се прилага, когато:

1.Предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2.Записването или разкриването на личните данни са изрично предвидени в закон;-

3.Физическото лице, за което се отнасят данните, вече разполага с информацията по ал.1.

Право на достъп до лични данни

Чл. 24. (1) Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

а) целите на обработването;

б) съответните категории лични данни;

в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

д) когато е приложимо, съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

е) правото на жалба до надзорен орган;

ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

з) съществуването на автоматизирано вземане на решения, включително профилиране и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

(2)Администраторът предоставя безплатно копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна такса въз основа на административните разходи. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго.

Право на коригиране на данни

Чл.25. Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез добавяне на декларация.

Право на изтриване (право „да бъдеш забравен“)

Чл.26.(1) Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

в) субектът на данни упражни право на възражение съгласно член 21, параграф 1 от Регламент (ЕС) 2016/679 /когато данните се обработват в изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора и обработването е необходимо за целите на легитимните интереси на администратора или на трета страна/ и няма законни основания за обработването, които да имат преимущество;

г) личните данни са били обработвани незаконосъобразно;

д) съществува нормативно задължение на администратора за изтриване на данните

(2) ал.1 не се прилага, доколкото обработването е необходимо:

а) за упражняване на правото на свобода на изразяването и правото на информация;

б) за спазване на правно задължение, което изисква обработване, предвидено в правото европейското или национално законодателство, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

в) за целите на архивирането в обществен интерес,

г) за установяването, упражняването или защитата на правни претенции.

Право на ограничаване на обработването

Чл. 27 (1). Субектът на данните има право да изиска от администратора ограничаване на обработването, когато е налице едно от следните условия:

а) точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на личните данни;

б) обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

в) администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

г) субектът на данните е възразил срещу обработването и е в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

(2) Когато обработването бъде ограничено, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице или поради важни основания от обществен интерес за Съюза или държава членка.

Право на преносимост на данните

Чл.28 (1) Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато са налице следните условия:

а) обработването е основано на съгласие на субекта на данните за обработване на личните му данни за една или повече конкретни цели или на договорно задължение

и

б) обработването се извършва по автоматизиран начин.

(2) Когато упражнява правото си на преносимост на данните по ал. 1, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

Право на възражение

Чл. 29 (1) Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, но само в случаите когато неговите данни се обработват на основание: необходимо за целите на легитимните интереси на администратора или на трета страна, съгласно чл.6, б.“е“ от Регламента.

(2) Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

(3) Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото по ал.1 и ал.2, което му се представя по ясен начин и отделно от всяка друга информация.

ПРОЦЕДУРИ

Чл. 30 (1) Правото на достъп по чл. 24 и правата по чл. 25, чл.26, чл. 27, чл.28 и чл. 29, се осъществяват с писмено заявление до администратора на лични данни.

(2) Заявление може да бъде отправено и по електронен път, по реда на Закона за електронния документ и електронния подпис.

(3) Заявлението се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно. Заявлението следва да съдържа законоизискуемите реквизити по чл. 30 от ЗЗЛД, като при подаване чрез пълномощник се прилага и нотариално заверено пълномощно.

(4) Заявленията по чл. 30 се завеждат в регистър от администратора.

Чл. 31. (1) Информацията по чл. 24, ал. 1 може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(2) Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон. Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

Чл. 32. (1) В случаите по чл. 24, ал. 1 администраторът на лични данни или изрично оправомощено от него лице разглежда заявлението по чл. 30 и се произнася в 14-дневен срок от неговото подаване.

(2) Срокът по ал. 1 може да бъде удължен от администратора или от изрично оправомощено от него длъжностно лице до 30 дни в уредените от ЗЗЛД случаи, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(3) В 14-дневен срок администраторът или изрично оправомощено от него длъжностно лице взема решение за предоставянето на пълна или частична информация по чл. 24, ал. 1 на заявителя или мотивирано отказва предоставянето й.

Чл. 33 (1) В случаите по чл. 25, чл.26, чл. 27, чл.28 и чл. 29, администраторът или изрично оправомощено от него длъжностно лице взема решение и извършва съответното действие в 14-дневен срок от подаване на заявлението по чл. 30 или мотивирано отказва извършването му.

(2) Когато е приложимо, едновременно с решението по ал.1 администраторът или изрично оправомощено от него длъжностно лице уведомява и трети лица: обработващия данни, когато е приложимо или външни партньори /фирми за правни, счетоводни, IT услуги и др./ за извършване на определени действия във връзка с изпълнение на решението по ал.1.

Чл. 34. **(1)** Администраторът на лични данни или изрично оправомощено от него длъжностно лице писмено уведомява заявителя за решението или отказа си по чл. 32 и чл. 33, в съответния срок.

(2) Уведомяването по ал. 1 е лично срещу подпис или по пощата с обратна разписка.

IV.Уведомяване на надзорния орган и субекта на данни за нарушение на сигурността на личните данни. Констатиране на нарушения

Чл. 35 (1) Нарушение на сигурността на лични данни съставлява нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

(2) Нарушенията по ал.1 се констатират:

1. Служебно от Управителя, при изпълнение на функциите и задълженията му;

2. По сигнал на служител до управителя. Сигналът следва да бъде подаден незабавно след откриване на нарушението от служителя.

3. По сигнал на външен източник- обработващ данни- когато е приложимо; външни партньори /фирми за правни, счетоводни, IT услуги и др./.

(3) Администраторът 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.

(4) За нарушенията Администраторът може да води дневник, в който да се вписват предполагаемото време или период на настъпване, описание на нарушението, времето на установяване, времето на докладване и името на лицето, подало сигнала.

(5) Администраторът, без ненужно забавяне, извършва анализ на фактите и обстоятелствата по сигнала и при наличие на нарушение то се констатира, като се вписва в дневника нарушението, последствията от нарушението и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява незабавно, като това се отразява в дневника.

(6) Когато е необходимо Администраторът издава и предписание до служители или трети лица за последващи действия във връзка с отстраняване на нарушението и/или на

последствията от нарушението. Предписанието се връчва без ненужно забавяне, но не по-късно от 3 /три/ дни от издаването му, на всички заинтересовани служители на дружеството или трети лица.

Чл.36 (1) 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 личните данни надзорния орган. Уведомление не се дължи само, ако не съществува вероятност нарушението на сигурността да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(2). Уведомлението по ал.1 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 на лице за контакт, от който 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.

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

Чл. 37 (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, посочено ал. 1, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в член 36, ал.2 букви б), в) и г).

(3) Посоченото в ал. 1 съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

а) администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по- специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

в) то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

(4) Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията на ал.3

V.Вътрешни мерки за превенция, защита и преустановяване на нарушения на нормативните актове при обработване на лични данни

Чл.38 (1) Незаконосъобразно обработване на данни или неспазване на нормативните изисквания на европейското и национално законодателство при обработване на лични данни, при осъществяване дейността на Администратора се констатират:

1. Служебно от Управителя, при изпълнение на функциите и задълженията му;

2. По сигнал на служител при откриване на нарушение или при съмнение за подобно нарушение. Сигналът се подава до Управителя без ненужно забавяне след откриване на нарушението или възникване на съмнение у служителя.

(2) Администраторът извършва без ненужно забавяне анализ на фактите и обстоятелствата по сигнала и при наличие на нарушение, го констатира. За нарушенията Администраторът води дневник, в който задължително се вписват: описание на нарушението, предполагаемото време или период на извършване, фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него, времето на установяване, времето на докладване и името на лицето, подало сигнала.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ:

§ 1. За неуредените от тази Инструкция въпроси се прилагат разпоредбите на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016, Закона за защита на личните данни /ЗЗЛД/ и Инструкция №1/30.01.2013г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, като при противоречие на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 с националното законодателство се прилагат разпоредбите на Регламента.

§2.Настоящата Инструкция влиза в сила от датата на утвърждаването и се прилага от 25.05.2018г., като може да бъде изменяна при промяна на действащата нормативна уредба.