УТВЪРЖДАВАМ:

Минна Станева, Управител

ИНСТРУКЦИЯ
за мерките за защита на личните данни в ПРИНТ СОЛЮШЪНС ЕООД

I. Общи положения

Предмет

Чл. 1. Тази инструкция урежда условията и реда за водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни в Принт салюшънс ЕООД.

Принципи при обработване на лични данни

Чл. 2. При обработването на лични данни в Принт Солюшънс ЕООД се спазват следните принципи:

1. законосъобразност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхранението;
6. цялостност и поверителност;
7. отчетност.

II. Администратор и регистри с лични данни

Индивидуализиране на администратора на лични данни

Чл. 3. (1) Администратор на лични данни е Принт солюшънс ЕООД, със седалище и адрес на управление: Русе 7002 бул. Цар Освободиштел 1 вх. А. Адресът за кореспонденция и контакт е Русе 7005 бул. Липник 129 , тел. 0888343487.

(2) Администраторът обработва лични данни във връзка с НОИ, НАП, банки, митница, куриери, застрахователни дружества, МВР, обработка на болнични листи, като определя сам целите и средствата за обработването им, при спазване на относимите нормативни актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни и чрез възлагане на обработващи лични данни.

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

Условия за достъп до лични данни

Чл. 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, до които са получили достъп при и по повод изпълнение на задълженията си.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Чл. 5. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;

2. целите на обработването на личните данни и правното основание за обработването;

3. категориите лични данни, отнасящи се до съответното физическо лице;

4. получателите или категориите получатели, на които могат да бъдат разкрити данните;

5. срока за съхранение на личните данни;

6. информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 – Общия регламент относно защитата на данните;

7. право на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8. правото на жалба до надзорен орган – за Република България Комисията за защита на личните данни;

9. източника на данните;

10. съществуване на автоматизирано вземане на решения, включително профилиране.

(2) Алинея 2 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването или разкриването на данни са изрично предвидени в закон;

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

4. е налице изрична забрана за това в закон.

Поддържани регистри на лични данни

Чл. 6. В Принт солюшънс ЕООД се обработват лични данни в следните регистри:

1. Регистър Персонал“ и

2. Регистър „Пропускателен режим“.

III. Регистър „Персонал“

Общо описание на регистъра

Чл. 7. В регистъра се обработват лични данни на кандидатите за работа и на служителите, работниците и изпълнителите по граждански договори с оглед:

1. индивидуализиране на трудови, служебни и граждански правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за Националния архивен фонд и др.;

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

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

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

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

г) за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови и служебни правоотношения и граждански договори.

Категории лични данни, обработвани в регистъра

Чл. 8. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

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

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. икономическа идентичност: данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др.;

5. лични данни относно гражданскоправния статус на лицата, необходими за длъжностите, свързани с материална отговорност (напр. свидетелства за съдимост);

6. данни за здравословното състояние (медицинско свидетелство при постъпване на работа, периодични прегледи, преминавани с оглед характера на работата, изпълнявана по трудовото правоотношение и изискванията за безопасни условия на труд);

7. данни за членство в синдикални организации.

Технологично описание на регистъра

Чл. 9. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Данните в регистъра се предоставят от физическите лица при кандидатстване за работа в Принт солюшънс ЕООД . Данните се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(4) Данните в регистъра се съхраняват за срок от 50 години във връзка с нормативно установени срокове.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни.

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

Чл. 10. (1) Данните от регистъра се обработват от Минна Станева - Управител, в чиито длъжностна характеристика е определено задължение за обработване на данните на служителите и при спазване на принципа „Необходимост да се знае".

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на Регистър Персонал"

Чл. 11. (1) Оценка на въздействието на Регистър „Персонал" се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой надхвърля 100, но не надхвърля 10 000;

2. в регистъра се обработват специални категории лични данни, свързани със здравословното състояние на работниците и служителите и данни за членство в синдикални организации с оглед прилагане на изискванията на трудовото законодателство.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на Регистър „Персонал“ е средно.

(3) 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.

Оценка на нивото на въздействие на „Регистъра на служителите“

Наименование на регистъра	**НИВО НА ВЪЗДЕЙСТВИЕ**			
	поверителност	**цялостност**	**наличност**	**общо за регистъра**
Персонал	средно	средно	средно	средно

Технически и организационни мерки за защита на личните данни в Регистър „Персонал“

Чл. 12. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват в кабинетите на упълномощените по чл. 10 лица.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с ограничен достъп само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни се намират в заключен шкаф, в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра са оборудвани с заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

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

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. 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 кадровото досие на всеки служител.

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

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Персонал“ се поддържа на хартиен носител (кадрови досиета, чието съдържание съответства на нормативната уредба на Република България, както и на

вътрешните нужди за периодична оценка на служителите), а отделни дейности по обработване на данните в него налагат поддържане на данни в електронен вид.

2. Обработването на личните данни се извършва в рамките на работното време на Принт солюшънс ЕООД.

3. Достъп до регистъра имат лицата по чл. 10 в съответствие с принципа „Необходимост да се знае".

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Минна Станева е отговорна за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от Регистър „Персонал", които са на хартиен носител, са определени в чл. 9, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в Принт солюшънс ЕООД.

8. Архивирането на документи се възлага на Минна Станева при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Управителя на Принт солюшънс ЕООД комисия. Унищожаването се извършва след изрично писмено разрешение на Управителя.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на отдалечен сървър, намиращ се извън фирмата. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. 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, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3.Минна Станева е отговорна за управлението на регистъра. Само лицата посочени в чл. 10 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

6. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм.

7. Контролът по използването на тези носители се осъществява от Минна Станева.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от фирма Щит ЕООД в Русе и Бумеранг ЕООД в София;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 9, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните, както и използване на електронен подпис.

Действия за защита при аварии, произшествия и бедствия

Чл. 13. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Управителя, като това се отразява в дневника по архивиране и възстановяване на данни.

Предоставяне на лични данни на трети лица

Чл. 14. (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, Принт солюшънс ЕООД предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители и изпълнители по граждански договори. Личните данни, който се предоставят, са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови преводи.

(3) Във връзка с използването на куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица Принт солюшънс ЕООД посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 15. Управителят трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 16. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за Принт солюшънс ЕООД, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

IV. Регистър „Пропускателен режим“

Общо описание на регистъра

Чл. 17. В регистъра се обработват лични данни на лица, които влизат в сградата и прилежащите имоти на администратора на адрес Русе 7002 бул. Липник 129 и София 1784 бул. Цариградско шосе 117 и са необходими за осъществяване на частна охранителна дейност за следните цели:

1. индивидуализиране на влизащите лица;
2. установяване на периода на достъпа до сградите и охранявания периметър.

Категории лични данни, обработвани в регистъра

Чл. 18. В регистъра се обработват следните категории лични данни:

1. физическа идентичност: имена и номер на документ за самоличност;
2. записи от наблюдение чрез технически средства.

Технологично описание на регистъра

Чл. 19. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Данните в регистъра се предоставят от физическите лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Данните в регистъра се съхраняват за срок съгласно с нормативно установени срокове.

(5) Администраторът на лични данни предоставя достъп, справки, извлечения, издаване на документи и други услуги от съответния регистър с лични данни, ако е предвидено в нормативен акт.

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

Чл. 20. (1) Данните от регистъра се обработват чрез обработващ данни, а именно Минна Станева, в договора с който е възложено обработването при спазване на всички изисквания за защита на личните данни и прилагане на принципа „Необходимост да се знае”.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието на регистър „Пропускателен режим“

Чл. 21. (1) Оценка на въздействието на регистър „Пропускателен“ се извършва в съответствие с критериите по чл. 11, ал. 2 във връзка с чл. 14 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, при съобразяване със следните обстоятелства:

1. в регистъра се обработват лични данни за лица, чийто брой не надхвърля 10 000;
2. в регистъра се обработват лични данни с автоматизирани средства;
3. в регистъра не се съдържат специални категории лични данни.

(2) При отчитане на критериите по ал. 1, нивото на въздействие на регистър „Лични данни на лица, подали молби, жалби, предложения“ е ниско.

(3) 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.

Оценка на нивото на въздействие на регистър „Пропускателен режим“

Наименование на регистъра	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	цялостност	наличност	общо за регистъра
Пропускателен режим	ниско	ниско	ниско	ниско

Технически и организационни мерки за защита на личните данни в регистър „Пропускателен режим“

Чл. 22. (1) Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Личните данни от регистъра се обработват от обработващ лични данни.

2. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове в кабинет с ограничен достъп само за упълномощени лица.

3. Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

4. Помещенията, в които се обработват лични данни от регистъра, са оборудвани с заключване на вратите и пожарогасителни средства.

5. Физическият достъп до зоните в обекта с ограничен достъп, включително и тези, в които са разположени елементи на комуникационно-информационните системи, е възможен само през заключващи се врати. Достъп се предоставя само на служителите, чийто служебни задължения включват обработване на лични данни от регистъра.

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

(2) Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със ЗЗЛД, Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, настоящата Инструкция и правилата за информационна сигурност при постъпване на работа.

2. Лицата, обработващи лични данни, преминават обучение, включващо запознаване с политиката и ръководствата за защита на личните данни, запознаване с опасностите за личните данни, обработвани от администратора, като се провежда тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

3. 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 кадровото досие на всеки служител.

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

(3) Документалната защита на обработваните в регистъра лични данни се осъществява при спазване на следните мерки:

1. Регистър „Пропускателен режим“ се поддържа на хартиен носител (книги за достъп.).

2. Обработването на личните данни се извършва в рамките на работното време на Принт солюшънс ЕООД.

3. Достъп до регистъра имат лицата по чл. 20 в съответствие с принципа „Необходимост да се знае”.

4. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Данните се класифицират в съответствие с тяхното

предназначение и характер и се съхраняват в заключващ се шкаф в зоните с ограничен достъп.

5. Минна Станева е отговорен за контрол на достъпа до регистъра.

6. Сроковете за съхранение на документи от регистъра които са на хартиен носител, са определени в чл. 19, ал. 4.

7. Документите се съхраняват в отредените за целта служебни помещения в Принт солюшънс ЕООД.

8. Архивирането на документи се възлага на Минна Станева при спазване на съответните защитни мерки за определеното ниво на защита.

9. Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.

10. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер).

11. След изтичане на срока за съхранение документите от регистъра се унищожават чрез нарязване или изгаряне, за което се съставя протокол от назначена със заповед на Управителя комисия. Унищожаването се извършва след изрично писмено разрешение на Минна Станева.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистъра се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър, намиращ се в офис София. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. 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, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. Минна Станева е отговорен за управлението на регистъра. Само лицата посочени в чл. 20 имат достъп до регистъра.

4. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

5. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа, сигнално-охранителна система.

6. Всички технически носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорна каса със заключващ механизъм.

7. Контролът по използването на тези носители се осъществява от Минна Станева.

8. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата с денонощна охрана, осъществявана от охранителна фирма Щит ЕООД в Русе и Бумеранг ЕООД в София;

б) Забранено е използването на преносими лични носители на данни.

в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

9. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

10. Сроковете за съхранение на данни от регистъра са описани в чл. 19, ал. 4.

(5) Криптографската защита при предаване на данни по електронен път или на преносими технически носители се осъществява чрез използване на стандартни технологии за криптиране на данните.

Действия за защита при аварии, произшествия и бедствия

Чл. 23. (1) При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на Управителя, като това се отразява в дневника по архивиране и възстановяване на данни.

Предоставяне на лични данни на трети лица

Чл. 24. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и т.н.).

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 25. Управителят трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

Ред за изпълнение на задълженията по чл. 25 от ЗЗЛД

Чл. 26. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности за Принт солюшънс ЕООД, а именно: чрез разрязване с помощта на машина – шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни.

(3) В случай на прехвърляне на данните на друг администратор е необходимо да се уведоми КЗЛД, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването и се съставят съответно приемо-предавателни протоколи.

ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА

Параграф единствен. Инструкцията се приема на основание чл. 23, ал. 4 от Закона за защита на личните данни, чл. 19, т. 2 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и при спазване на сроковете по § 2 от Преходните и заключителни разпоредби на Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.