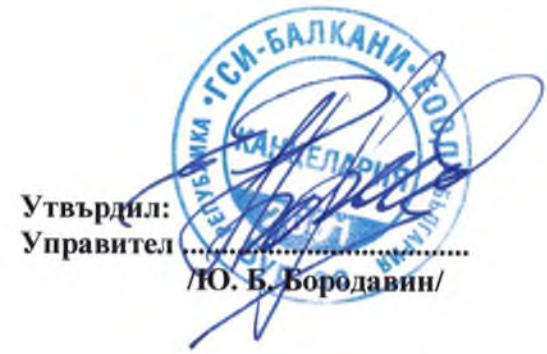
„ГСИ – БАЛКАНИ” ЕООД



Утвърдил:
Управител .....
/Ю. Б. Бородавин/

РАБОТНА ИНСТРУКЦИЯ

ЗА ПРИЛАГАНЕ НА ВЪТРЕШНИТЕ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В „ГСИ – БАЛКАНИ“ ЕООД

ПРЕДМЕТ

Тази Работна инструкция се приема, с цел правилното прилагане на Вътрешните правила за защита на личните данни в частност и Общия регламент за защита на данните (Регламент 2016/679).

ДЕФИНИЦИИ

Чл. 1. За целите на настоящата Работна инструкция, използваните понятия имат следното значение:

• **ЗЗЛД** – Закон за защита на личните данни.

• **КЗЛД** – Комисия за защита на личните данни.

• **ОРЗД** – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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).

• **Длъжностно лице по защита на данните** – физическо лице, определено съгласно изискванията на чл. 37 и сл. от ОРЗД.

• **Администратор на лични данни** – 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. В настоящите Правила „администратор“ обозначава Дружеството.

• **Обработващ лични данни** – лице или организация, което въз основа на договор обработва лични данни, предоставени от Дружеството, за уговорените цели.

• **Известия по защита на данните** – отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който Дружеството събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.

• **Обработване на данни** – всяка дейност, която е свързана с използването на лични данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на лични данни до трети лица.

• **Псевдонимизиране** – заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними"), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.

• **Съгласие** – всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 2. (1) Личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа, се събират при и по повод набирането на персонал, изпълнение на трудовите задължения, плащане на трудово възнаграждение, опазване на здравето на работниците.

Личните данни се събират на хартиен носител и/или на електронен носител при подаване на молба за работа или при промяна на обстоятелства и данни при вече назначени работници.

Събраните лични данни на всеки работник и служител на Дружеството се съхраняват в лични досиета, в поименни папки, като някои или всички данни могат да се съхраняват или обработват и на технически носител.

Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в зависимост от нуждата.

Информацията за кандидатите за работа се събира чрез попълване на утвърдени в дружеството формуляри и други документи.

Електронните данни се съхраняват в бази данни.

(2) Личните данни, отнасящи се до лицата, прекратили своите трудови или граждански правоотношения в Дружеството, се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. И тези електронни данни се съхраняват в бази данни.

Тези досиета се подреждат в нарочно обособена стая – архив, която се заключва и до нея имат достъп само Лицето, отговорно за личните данни и служителя в отдел „Правни и кадрови въпроси".

Тези лица са оправомощени да събират и обработват личните данни.

(3) Личните досиета се подреждат в специални картотечни шкафове със заключване, находящи се в кабинета на Лицето, отговорно за личните данни или в кабинета на служител от отдел „Правни и кадрови въпроси".

Данните на кандидатите за работа, ако има такива и които се съхраняват на хартиен носител, се съхраняват в нарочни шкафове в кабинета на Лицето, отговорно за личните данни или се съхраняват в нарочно обособена стая – архив, която се заключва и до която имат достъп само

Лицето, отговорно за личните данни и Специалист човешки ресурси в отдел „Правни и кадрови въпроси“.

(4) Достъпът до кабинетите на Лицето, отговорно за личните данни и Специалист човешки ресурси в отдел „Правни и кадрови въпроси“ е ограничен.

Освен Лицето, отговорно за личните данни и Специалист човешки ресурси в отдел „Правни и кадрови въпроси“, в кабинетите нямат право да влизат или да се намират външни лица (независимо дали са работници на дружеството или на са) без в същото време в съответния кабинет да се намира и Лицето, отговорно за личните данни или Специалист човешки ресурси.

При всички случаи, когато се наложи на Лицето, отговорно за личните данни или Специалист човешки ресурси да напусне кабинета си, независимо от причината и времето на отсъствието си, съответния кабинет се заключва, като се затварят и прозорците.

Чл. 3. (1) Личните данни, отнасящи се до размера на трудовите възнаграждения, социални придобивки, задължения към трети лица, обезпечителни мерки и др. подобни се събират на хартиен носител и/или на електронен носител.

(2) Тези лични данни, отнасящи се до лицата, прекратили своите трудови или граждански правоотношения в Дружеството, се съхраняват в досиета, като някои данни могат да се съхраняват или обработват и на технически носител.

Тези досиета се подреждат в нарочно обособена стая – архив, която се заключва и до нея имат достъп само Главния счетоводител, заместника му и служителите в отдел счетоводен. Тези лица са оправомощени да събират и обработват финансовите личните данни.

(3) Достъпът до кабинетите на Главния счетоводител, заместника му и служителите в отдел счетоводен е ограничен.

Освен тези лица, в кабинетите нямат право да влизат или да се намират външни лица (независимо дали са работници на дружеството или на са) без в същото време в съответния кабинет да се намира и Главния счетоводител или служител от отдел Счетоводен.

При всички случаи, когато се наложи на Главния счетоводител или на служител от отдел Счетоводен да напусне кабинета си, независимо от причината и времето на отсъствието си, съответния кабинет се заключва, като се затварят и прозорците.

Чл. 4. (1) Правилата и мерките по чл. 2 и чл. 3 важат и за останалите Лица, оправомощени да обработват лични данни.

Чл. 5. (1) Лицата, оправомощени да обработват лични данни, предприемат всички организационно – технически мерки за съхраняването и опазването на личните досиета и класьорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

Чл. 6. (1) В интерес на работата и когато това е необходимо за изпълнението на производствените задачи и по тяхна преценка, Лицата, оправомощени да обработват лични данни, по искане на съответните служители, им предоставят нужната им информация, съдържаща лични данни, за всеки конкретен случай.

Информация, съдържаща лични данни, освен лицата обработващи лични данни, имат право да искат и съответно да получат: Управител, Главен инженер, Началници на управления, Началници на отдели и служби в администрацията.

(2) Искането е формално за всеки конкретен случай, отправя се до Лицето, отговорно за личните данни и съдържа: личните данни, които се искат, целта за която ще се ползват и подпис на служителя.

(3) Въпросните служители използват информацията строго за нуждите, за които са я поискали, при спазване на същите мерки за сигурност, каквито са вменени на Лицата, оправомощени да обработват лични данни и каквито са описани в тези правила. След като приключат с работата с предоставените им лични данни, въпросните служители по правило или

унищожават данните или ги предават обратно на Лицата, оправомощени да обработват лични данни.

(4) В интерес на работата и в случай, че се налага служителите да съхранят част или цялата предоставена им информация, за определено време, те следва да положат предвидената в тези правила грижа за тази информация.

Кабинетите на тези лица следва да са оборудвани със заключваеми шкафове или каси, както и с други средства, предвидени във вътрешните правила и тази инструкция.

Чл. 7. (1) Досиета на работниците и служителите, данните на кандидатите за работа, както и всички други лични данни, които се обработват в дружеството не се изнасят извън сградата на дружеството.

Чл. 8. (1) Личните данни, отнасящи се до клиенти, се събират при подаване на заявка за предоставяне на услуга или сключване на договор с клиент на Дружеството.

(2) Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори.

(3) Личните данни се съхраняват на електронен и хартиен носител (подписани оригинали на сключените договори), които се класират в отделни досиета.

Досиетата се съхраняват в шкафове, които се заключват, в кабинета на Лицето, отговорно за личните данни или се съхраняват в нарочно обособена стая – архив, която се заключва и до която имат достъп само Лицето, отговорно за личните данни и служителя в отдел „Правни и кадрови въпроси“.

Електронните данни се съхраняват в бази данни.

Чл. 9. (1) Освен чрез гореописаните процедури личните данни, които се събират в дружеството се съхраняват и обработват и в лицензирана софтуерна система Microsoft Dynamics NAV.

Достъпът до софтуерната система Microsoft Dynamics NAV имат само определен брой служители, всеки от които има достъп само до определен модул от системата.

(2) Достъпът на всеки от гореизброените служители е защитен с парола.

(3) Служителите, които имат достъп до софтуерната система Microsoft Dynamics NAV работят в нея само в своите кабинети и на своите компютри и не допускат външни лица в кабинета.

Ако външен човек влезе в кабинета по време когато съответния служител работи в системата, последния е длъжен или да минимизира екрана или да изключи системата докато външния човек излезе от кабинета, като не даде никакъв шанс за изтичане на информация от Microsoft Dynamics NAV.

(3) Служителите, които имат достъп до софтуерната система Microsoft Dynamics NAV не копират данни от нея без разрешение на Лицето, отговорно за личните данни.

Искането е съгласно чл. 6, ал. 2 от тази инструкция.

Чл. 10. (1) В електронния сървър на дружеството, в папките със свободен достъп, не се допуска поставянето на документи, съдържащи лични данни.

(2) Документи, съдържащи лични данни, могат да се поставят единствено в т.нар. „поверителни папки“, които са защитени с пароли и достъп до които имат строго определен брой лица. В тези папки документи, съдържащи лични данни могат да поставят само Лицето, отговорно за личните данни или Лицата, оправомощени да обработват лични данни.

Чл. 11. (1) Лицата, оправомощени да обработват лични данни не държат върху бюрата си документи, съдържащи лични данни, когато в кабинета се намират външни лица.

(2) Когато в кабинета на Лице, оправомощено да събира лични данни влезе външен човек, то предприема мерки за скриване на документите, които съдържат лични данни.

ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТКАТА И СЪХРАНЕНИЕТО НА ЛИЧНИТЕ ДАННИ И ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 12. (1) Лицето, отговорно за личните данни, и лицата, обработващи личните данни от името на дружеството, са служители в дружеството, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите Правила.

(2) Лицето, отговорно за личните данни:

- подпомага Дружеството и лицата, обработващи личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;
- осигурява нормалното функциониране на гореспоменатите системи за защита;
- осъществява контрол през целия процес на събиране и обработване на данните;
- изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;
- периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;
- уведомява Дружеството своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;
- унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези Правила;
- преупълномощава физически или юридически лица с писмен акт, които да осъществяват защитата на личните данни.

(3) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

(4) Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др.

Гореспоменатите могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

(5) В „ГСИ – БАЛКАНИ“ ЕООД право да обработват лични данни, съобразно предходните членове имат следните служители:

- Длъжностно лице по защита на личните данни – Радомир Йорданов Вълчев, Началник отдел „Правни и кадрови въпроси“.
- Лица оправомощени да обработват лични данни:
  Детелина Митрева – Специалист „Човешки ресурси“;
  Иван Карагьозов – Главен счетоводител;
  Анна Букурова – Началник служба „ФиК“, зам. главен счетоводител;
  Иван Тодоров – Счетоводител;
  Красимир Ковчезлиев – Счетоводител;
  Йовчо Йовчев – Началник отдел „Транспорт и механизация“;
  Димитър Динков – Началник отдел „Промишлена безопасност“;
  Стойка Джапарова – Офис меноджър.

(6) Лицата, оправомощени да обработват лични данни, извършват тази дейност в рамките на своите компетентности и за целите на изпълнение на трудовите си задължения.

(7) Длъжностното лице по защита на личните данни в рамките на своите правомощия контролира цялостната организация по защита на данните и в тази връзка издава предписания, указания и разпореждания, които имат задължителен характер за персонала.

НИВА НА ВЪЗДЕЙСТВИЕ, НИВА НА ЗАЩИТА И РЕГИСТРИ

Чл. 13. (1) Според характера на обработваните лични данни, в дружеството се определят следните нива на въздействие и съответните нива на защита на личните данни:

- Ниско ниво на въздействие и съответното му ниско ниво на защита. Имат се предвид случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Това са личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа, се събират при и по повод набирането на персонал, в това число:

- Име, адрес, телефонен номер и имейл адрес;
- Дата на раждане;
- Номер и дата на издаване на лична карта;
- Пол;
- Семейно положение и деца (в определени случаи: лични данни на съпруг/съпруга и други близки за упражняване на трудови права, напр. при отпуски по майчинство);
- Информация за банкови сметки;
- Информация за трудовия стаж и професионалния Ви опит (включително заемани длъжности, работно време, стаж по специалността, членство в професионални и съсловни организации);
- Размер на трудово възнаграждение, социални придобивки, задължения към трети лица, обезпечителни мерки;
- Месторабота;
- Номер, дата на издаване и категория на шофьорска книжка, в случай, че се налага да управлявате служебен автомобил;
- Информация относно притежавани квалификации, правоспособности, сертификати;
- Информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочена във Вашата автобиография и придружително писмо или предоставена по друг начин чрез процеса на кандидатстване);
- Атестационна информация;
- Информация относно трудова дисциплина;
- Записи от системи за видеонаблюдение, както и друга информация, получена по електронен път като например информация от електронни карти за достъп;
- Информация за употребата от Ваша страна на нашите информационни и комуникационни системи;
- Снимки;
- Членство в синдикални организации;
- Информация за наказателни присъди и нарушения, само ако се изисква от закон.

- Средно ниво на въздействие и съответното му средно ниво на защита. Имат се предвид случаите, когато неправомерното обработване на лични данни би могло да създаде

опасност от засягане на интереси, разкриващи здравословното състояние на титуляря на личните данни.

Това са личните данни, отнасящи се до лицата, заети по трудови или граждански правоотношения в Дружеството, както и на кандидатите за работа, се събират при и по повод набирането на персонал, в това число:

- Информация за здравословно състояние;
- Биометрични данни.

Чл. 14. (1) Дружеството поддържа регистрите по чл. 4, ал. 1 от ВПЗЛД с лични данни, съгласно предходната алинея и извършва оценка на въздействие за тях, съгласно Приложение № 1.

ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 15. (1) Дружеството документира дейностите по обработване на лични данни при спазване на принципа на отчетност.

(2) Документацията се съхранява при Длъжностното лице по защита на личните данни.

(3) Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните, се документира чрез създаване на протоколи, които съдържат следната информация:

(а) целите на обработването;

(б) категориите лични данни и категориите субекти на данни;

(в) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;

(г) предаването на лични данни на трета държава;

(д) когато е възможно, предвидените срокове за изтриване на различните категории данни;

(е) общо описание на техническите и организационни мерки за сигурност.

(4) Протоколите се изготвят от лицата, които извършват съответната обработка на данни по указания от Лицето, отговорно за личните данни.

(5) Съвкупността от всички протоколи, съдържащи гореописаната информация, съставлява регистъра на дейностите по обработването, съгласно чл. 30 от ОРЗД.

МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Технически мерки

Чл. 16. (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа.

(2) Административната сграда на дружеството и всички производствени помещения се охраняват от фирма „Гард Ейч Ем Ес“ ЕАД.

(3) Освен това административната сграда и нейните входове и изходи се наблюдават с видеокамери, които контролират достъпа до помещенията.

(4) Всички стаи в административната сграда се заключват и не се оставят отключени без надзор.

(5) Помещенията, в които се съхраняват и обработват лични данни са снабдени с пожарогасители, метални шкафове с ключалки, обикновени шкафове с ключалки.

(6) Външни лица в помещенията на дружеството се допускат само с придружител от персонала.

(7) В административната сграда на дружеството са обособени специални помещения – архиви, които се заключват и до тях достъпът е силно ограничен.

Мерки за документална защита

Чл. 13. (1) Дружеството установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители при възникнала необходимост.

Персонални мерки на защита

Чл. 14. (1) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни попълват декларация, съгласно чл. 14 от Вътрешните правила за защита на личните данни.

(2) При постъпване на работа всички служители преминават обучение/инструктаж за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на дружеството, свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Обучението/инструктажа се провежда от Длъжностното лице по защита на личните данни и се документира в нарочен Дневник.

(3) Веднъж годишно се провеждат последващи обучения/инструктажи на персонала, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им. Последващите обучения/инструктажи се провеждат от Длъжностното лице по защита на личните данни и се документират в нарочни Дневници по структури.

Мерки за защита на автоматизирани информационни системи и криптографска защита

Чл. 15. (1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

Създават се т.нар. поверителни папки, в които може да се поставя информация, която ще е достъпна само за конкретен брой лица.

(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени (firewalls) и др.

(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.

Чл. 16. (1) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия и др., се осигурява посредством:

- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).

(2) Лицето, отговорно за личните данни, докладва минимум веднъж на шест месеца на ръководството на дружеството предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

Чл. 17. (1) Минималното ниво на технически и организационни мерки, описани в предходните текстове, са систематизирани в Приложение № 2.

НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 18. (1) При признаци за нарушение на сигурността на данните се процедира съгласно чл. 17 – чл. 19 от Вътрешните правила за защита на личните данни.

ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 19. (1) Дружеството може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор.

(2) В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на обработващ, Дружеството:

а/ изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;

б/ сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;

в/ информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:

а/ Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;

б/ Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;

в/ Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове, или

г/ Трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

(4) Дружеството не предоставя лични данни на трети лица, с които няма сключен договор и които не са негови клиенти или доставчици на услуги на обработващ.

УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 20. (1) Унищожаване на личните данни се извършва от Длъжностното лица по защита на личните данни, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина.

Електронните данни се изтриват от електронната база данни по начин, не позволяващ възстановяване на информацията.

ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 21. (1) Правата на субектите на данни са регламентирани в чл. 26 от Вътрешните правила за защита на личните данни.

Настоящата Работна инструкция е приета и влиза в сила в деня на подписването й.

Съгласувал: .....

Началник отдел „Правни и кадрови въпроси“

Приложение № 1

Към Работна инструкция към ВПЗЛД

Оценка на нивото на въздействие на регистър

	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	**цялостност**	**наличност**	**Общо за регистъра**
Име на регистъра				

Приложение № 2
към Работна инструкция за прилагане на ВПЗЛД

видове защити / нива на защита	физическа		персонална	документална	автоматизирани информационни системи и/или мрежи		криптографска
	организационни мерки	технически мерки	организационни мерки	организационни мерки	организационни мерки	технически мерки	технически мерки
ниско	* определяне на помещенията, в които ще се обработват лични данни; * определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; * определяне на организацията на физическия достъп;	*ключалки; * шкафове; * пожарогасителни средства; * оборудване на помещенията;	* познаване на нормативната уредба в областта на защитата на личните данни; * знания за опасностите за личните данни, обработвани от администратора; * съгласие за поемане на задължение за неразпространение на личните данни;	* определяне на регистрите, които ще се поддържат на хартиен носител; * определяне на условията за обработване на лични данни; * регламентиране на достъпа до регистрите; * определяне на срокове за съхранение; * процедури за унищожаване;	* персонална защита; * определяне на срокове за съхранение на личните данни; * процедури за унищожаване/заличаване/изтриване на носители;	* идентификация и автентификация; * управление на регистрите; * външни връзки/свързване; * защита от вируси; * копия/резервни копия за възстановяване; * носители на информация;	
средно	*** ниско ниво +** * определяне на използваните технически средства за физическа защита; * определяне на зоните с контролиран достъп;	*** ниско ниво**	*** ниско ниво +** * обучение; * споделяне на критична информация между персонала; * познаване на политиката и ръководствата за защита на личните данни; * тренировка на персонала за реакция при събития, застрашаващи сигурността на данните;	*** ниско ниво +** * контрол на достъпа до регистрите; * правила за размножаване и разпространение;	*** ниско ниво +** * физическа среда/ обкръжение;	*** ниско ниво +** * телекомуникации и отдалечен достъп; * поддържане/ експлоатация;	* стандартните криптографски възможности на операционните системи; * стандартните криптографски възможности на системите за управление на бази данни; *стандартните криптографски възможности на комуникационното оборудване;