РЕПУБЛИКА БЪЛГАРИЯ
Министерство на земеделието и храните
Изпълнителна агенция по сортоизпитване, апробация и семеконтрол

НАРЪЧНИК ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В съответствие с Регламент (ЕС) 2016/679 (GDPR)

В сила от: 25.05.2018 г.

Утвърдил: _____
инж. Бистра Павловска
Изпълнителен директор на ИАСАС

Съдържание

История на промените

Дата	Версия	Отговорен за промяната	Същност на промяната	Одобрил
26.01.2024	1.1	С. Стефанова	Стр. 12, 13 промяна на отговорното лице	
			Стр. 14 допълнена е информация за мястото, където заинтересованите лица могат да се запознаят с Ф 5-1.1 Политика за поверителност	
			Стр. 17 Допълване на отговорност и на IT специалист при оценяване и избор на подходящи технически мерки за защита на личните данни.	
			Стр. 18, 19 Промяна на наименованията на инструкции в специфични политики	

ГЛАВА 1. ВЪВЕДЕНИЕ

1.1. Цел

1.1.1. Настоящият Наръчник определя реда, изискванията и отговорностите в ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО СОРТОИЗПИТВАНЕ, АПРОБАЦИЯ И СЕМЕКОНТРОЛ (ИАСАС, Агенцията) по отношение на защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни.

1.1.2. Наръчникът въвежда изискванията на 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 и Закон за защита на личните данни, обн. ДВ. бр.1 от 4 Януари 2002 г. в ИАСАС.

1.1.3. За да докаже спазването на изискванията, ИАСАС в качеството си на администратор на лични данни, разработва, внедрява и поддържа документация за дейностите по обработване, за които носи отговорност.

1.2. Обхват

1.2.1 Принципите на защита на данните се прилагат към всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано.

Съгласно Европейската комисия,

"Лични данни" означава всяка информация, свързана с идентифицирано или идентифицируемо живо физическо лице. Отделни данни, които събирайки се заедно могат да доведат до идентифициране на конкретно лице, също представляват лични данни.

Лични данни, които са били деидентифицирани, кодирани или псевдонимизирани, но могат да бъдат използвани за повторно идентифициране на дадено лице, остават лични данни и попадат в приложното поле на Регламента.

Лични данни, които са станали анонимни по такъв начин, че лицето не е идентифицирано или вече не може да се идентифицира, вече не се считат за лични данни. За да бъдат данните действително анонимизирани, анонимността трябва да бъде необратима.

Примерите за лични данни включват:

- собствено име и фамилия;
- домашен адрес;
- имейл адрес, като например име.фамилия@дружество.com;
- номер на картата за самоличност;
- данни за местоположение (напр. функцията за данни за местоположение на мобилен телефон);
- адрес на интернет протокол (IP);
- идентификационен номер на "бисквитка";
- рекламния идентификатор на Вашия телефон;
- данни, съхранявани от болница или лекар, които биха могли да бъдат символ, който уникално идентифицира дадено лице.

Примерите за данни, които не се считат за лични данни, включват:

- регистрационен номер на дружество;
- имейл адрес, като например инфо@дружество.com;
- анонимни данни.

1.2.2. Защитата, предоставена с настоящия Наръчник се прилага за физическите лица, независимо от тяхното гражданство или местопребиваване, във връзка с обработването на техните лични данни от ИАСАС.

1.2.3. Ръководството на ИАСАС осъзнава отговорностите и задълженията си за всяко обработване на лични данни, извършено от Агенцията или от нейно име и въвежда и прилага подходящи и ефективни мерки, които отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица и е в състояние да докаже, че дейностите по обработване са в съответствие с настоящия регламент, включително ефективността на мерките.

1.2.4. ИАСАС обработва лични данни с автоматични (изцяло или частично) и с неавтоматични средства, както следва:

- Автоматичен начин на обработване – чрез електронни средства за записване и съхраняване на информация;
- Неавтоматичен начин на обработване – чрез подреждане на хартиен носител.

ГЛАВА 2. ОБЩИ ПОЛОЖЕНИЯ

2.1. Стратегия на ръководството относно защита на личните данни

Висшето ръководство на ИАСАС, в лицето на Изпълнителния директор, определя и поддържа **Стратегия за защита на личните данни** и гарантира нейния периодичен преглед и актуализация. Ръководството ясно декларира ангажиментите, които Агенцията поема по отношение на защитата на личните данни на физическите субекти, в ролята си на администратор/обработващ на лични данни.

Като одобрява и насърчава прилагането на политика за защита на личните данни, отразена в Наръчника, процедурите и инструкциите по защита на личните данни, Ръководството се ангажира да осигури съответствие със законодателството на ЕС и държавите членки по отношение на обработването на личните данни и защитата на "правата и свободите" на физическите лица, чиито лични данни ИАСАС събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

Към Наръчника по защита на личните данни са разписани процедури и други документи, в съответствие с всички приложими за дейността на Агенцията изисквания на Общия регламент. Регламент (ЕС) 2016/679 и настоящият Наръчник се прилагат по отношение на всички дейности по обработване на лични данни, включително тези, които съдържат лични данни на служители, клиенти, доставчици и партньори и всякакви други лични данни, които организацията обработва, получени от различни източници.

Настоящият Наръчник и Регистърът на дейностите по обработване и политиката се преглеждат и при необходимост актуализират при всяка настъпила промяна в дейностите на ИАСАС, изискванията или оценката на въздействието върху защитата на данните, но минимум веднъж годишно.

Ръководството на ИАСАС и Длъжностното лице по защита на личните данни осигуряват Регистърът на дейностите по обработване да се поддържа актуален и да бъде на разположение при поискване от надзорния орган.

Настоящият Наръчник и процедурите към него, са приложими за всички служители на ИАСАС и за външните изпълнители/контрагенти, извършващи обработване на лични данни от нейно име. Всеки служител, който нарушава вътрешните правила и политики, ще бъде обект на дисциплинарни действия, както и може да бъде обект на граждански или наказателни дела, ако поведението му нарушава закони или подзаконови актове.

Наръчникът по защита на личните данни може да се предоставя на външни изпълнители и трети лица, които работят с или за ИАСАС и които имат или могат да имат достъп до или обработват личните данни. Никоя трета страна няма достъп до лични данни, обработвани от ИАСАС, без да има сключен договор/споразумение за поверителност на данните, което налага на третата страна задължения при обработването на лични данни. Тези външни страни трябва да познават, разбират и прилагат изискванията на този Наръчник и съответните процедури и да доказват това съответствие при поискване от страна на ИАСАС, чрез попълване на въпросници за оценка и/или проверки на място.

ГЛАВА 3. ТЕРМИНИ И ОПРЕДЕЛЕНИЯ

"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;

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

"Профилиране" означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

"Псевдонимизация" означава обработване 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 с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

"Регистър с лични данни" означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

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

"Обработващ лични данни" означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

"Съгласие на субекта на данните" означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

"Нарушение на сигурността на лични данни" означава 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;

"Генетични данни" означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени по специфичен начин – от анализ на биологична проба от въпросното физическо лице;

"Биометрични данни" означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

"Данни за здравословното състояние" означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

"Дружество" означава физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, включително партньорствата или сдруженията, които редовно осъществяват икономическа дейност;

"Трансгранично обработване" означава или:

а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или

б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка;

ГЛАВА 4. ОТГОВОРНОСТИ И ПРАВОМОЩИЯ

4.1. Общи положения

Отговорността за осигуряване на подходяща обработка на лични данни се носи от всеки, който работи за или от името на ИАСАС и има достъп до обработваните от Агенцията лични данни. Основните сфери на отговорност при обработването на лични данни имат следните длъжности/отдели:

- Изпълнителният директор взема решения и одобрява общата стратегия на Агенцията за защита на личните данни;
- Длъжностното лице по защита на данните (ДЛЗД) отговаря за управлението на Наръчника по защита на личните данни, процедурите и формулярите към тях и за разработването и популяризирането на други документи, гарантиращи защита на личните данни, както е определено в т. 4.2. и в заповедта за възлагане на отговорности; одобряване на политика за поверителност;
- Юрисконсултът, съвместно с Длъжностното лице по защита на данните наблюдава и анализира законодателството в областта на личните данни и промените в него, разработва изисквания за съответствие и подпомага Агенцията в постигането на целите, свързани със защитата на личните данни;
- Системният администратор отговаря за:
  - осигуряване на всички системи, услуги и оборудване, използвани за съхранение на данни, да бъдат в съответствие с приемливи стандарти за сигурност;
  - провеждане на редовни проверки и сканиране, за да се гарантира, че хардуерът и софтуерът за защита функционират правилно.
- Служителят човешки ресурси /администрация отговаря за:
  - защита на личните данни на служителите, като гарантира, че личните данни на служителите се обработват въз основа на законните бизнес цели и нужди на работодателя.
- Директор административно и финансово обслужване отговаря за:

- осигуряване на експертни познания за защита на личните данни и обучение за повишаване на информираността на служителите, работещи с лични данни;
- предаване на отговорностите за защита на личните данни на доставчиците;
- повишаване на нивата на информираност на доставчиците за защита на личните данни;
- свеждане на изискванията за защита на лични данни към трети страни, които Агенцията използва;
- запазване правото на Агенцията да извършва проверки (одити) на доставчици.

4.2. Длъжностно лице по защита на данните (ДЛЗД)

4.2.1. Ръководството на ИАСАС със заповед определя Длъжностно лице по защита на данните, на което възлага функции и отговорности, свързани със защитата на личните данни, контрол по прилагането на цялостната Стратегия, Наръчника, Процедурите и Регламента в организацията и повишаването на осведомеността и компетентността на служителите. Допуска се ДЛЗД да бъде външно за Агенцията физическо лице, което изпълнява функциите въз основа на сключен договор за услуга.

4.2.2. Ръководството осигурява, че определеното Длъжностно лице по защита на личните данни притежава професионални качества и задълбочени експертни познания в областта на законодателството и практиката на защитата на личните данни.

4.2.3**.** Длъжностното лице по защита на личните данни има следните отговорности и пълномощия:

- да информира и консултира ръководството и служителите, които извършват обработване, за техните задължения, в съответствие с настоящите правила и приложимите нормативни актове за защита на личните данни;
- да наблюдава и контролира спазването на правилата за защита на личните данни и на Наръчника и процедурите/инструкциите по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в дейностите по обработване;
- да участва/консултира при оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
- да си сътрудничи с надзорния орган, при необходимост;
- да осъществява комуникация с надзорния орган по въпроси, свързани с обработването на лични данни, включително предварителната консултация.

При изпълнението на своите задачи Длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

4.2.4**.** Данните за контакт с Длъжностното лице по защита на данните се публикуват на сайта на ИАСАС и се съобщават на надзорния орган**.**

4.2.5**.** Ръководството на ИАСАС гарантира, че Длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни. Изпълнителният директор подпомага изпълнението на възложените отговорности, като осигурява необходимите за тях ресурси, достъп до личните данни и операциите по обработване, както и поддържане на експертните знания.

4.2.6. Ръководството гарантира, че Длъжностното лице по защита на данните няма да получава никакви указания във връзка с изпълнението на своите отговорности, както и че няма да бъде освобождавано от длъжност, нито санкционирано за изпълнението на своите задачи.

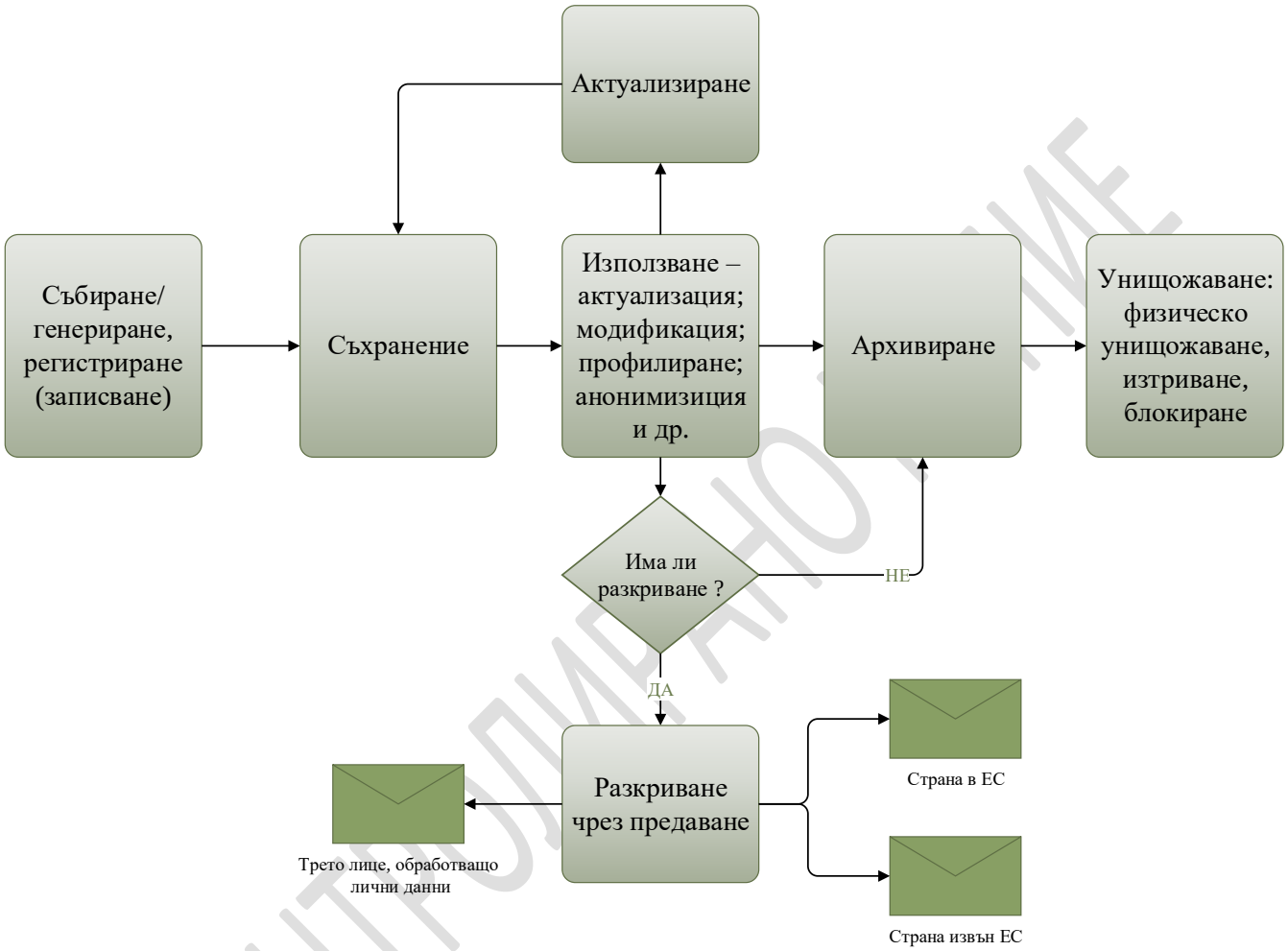
4.2.7. Ръководството на ИАСАС декларира, че наличието на други задачи и задължения на Длъжностното лице не водят до конфликт на интереси.

4.2.8. Физическите лица (субекти на данни) могат да се обръщат към Длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия Наръчник и Регламент (ЕС) 2016/679.

ГЛАВА 5. ИЗГРАЖДАНЕ НА ЗАЩИТА В БИЗНЕС ДЕЙНОСТИТЕ. ЖИЗНЕН ЦИКЪЛ НА ЛИЧНИТЕ ДАННИ

За да докаже съответствие с принципите за обработване на данните, ИАСАС прилага редица мерки за защита на данните, които е интегрирала в своите бизнес дейности.

Жизнен цикъл на личните данни



5.1. Уведомяване на субектите на данни

ИАСАС предприема необходимите мерки за предоставяне на всякаква информация и на всякаква комуникация, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и леснодостъпна форма, на ясен и прост език, като за целта изготвя **Ф 5-1.1 Политика за поверителност**.

Редът за информиране на субекта на лични данни е разписан в **П 5-1 Прозрачност на обработването**.

5.2. Избор и съгласие на субекта на данни

ИАСАС предоставя на субекта на данни правото на избор за даване на съгласие и за неговото оттегляне.

Редът за получаване на съгласие от субекта на лични данни е разписан в т 7.3. на настоящия Наръчник.

5.3. Събиране

Ръководството и ДЛЗД осигуряват, че ИАСАС няма да събира информация, която не е строго необходима за целта, за която тя е получена.

Агенцията се стреми да събира възможно най-малко количество лични данни. Ако личните данни се събират от трета страна, ръководството и ДЛЗД трябва да гарантират, че личните данни се събират законосъобразно.
ДЛЗД преглежда всички начини на събиране на данни минимум веднъж годишно, за да се гарантира, че събраните данни продължават да бъдат адекватни, подходящи и тяхното събиране продължава да бъде необходимо.

5.4. Използване, съхранение, архивиране и унищожаване
Целите, методите, ограниченото съхранение и периодът на запазване на личните данни са в съответствие с информацията, съдържаща се във **Ф 5-1.1 Политика за поверителност**. Агенцията поддържа точността, целостта, поверителността и уместността на личните данни въз основа на целите на обработването.
В ИАСА са създадени механизми за защита, предотвратчване на кражба или злоупотреба с лични данни и предотвратяване нарушаване на тяхната сигурност.
Когато личните данни се запазват след тяхното обработване, те се съхраняват по подходящ начин (минимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение сигурността на данните.
Личните данни се пазят в съответствие с **П 5-3 Съхранение и запазване на лични данни** и след изтичане на срока им на съхранение се унищожават по определения в **П 5-3** ред.
ДЛЗД писмено одобрява всеки случай на възникнала необходимост от запазване на данни за срок, по-дълъг от определения в **П 5-3 Съхранение и запазване на лични данни,** като гарантира, че обосновката е ясно определена и е в съответствие с нормативните изисквания, ако има такива.

5.5. Предоставяне и разкриване пред трети страни
Когато се възлага обработване на обработващ лични данни, ИАСАС използва само обработващи лични данни, които предоставят достатъчни гаранции по отношение на експертни знания, надеждност и ресурси, както и че ще бъдат предприети технически и организационни мерки, които отговарят на изискванията на настоящите правила и Регламент (ЕС) 2016/679, включително на изискванията за сигурността на обработването. Редът за управление на лицата, обработващи лични данни от името на ИАСАС, е определен в **П 5-4 Взаимоотношения с доставчици**.
ИАСАС разкрива лични данни на публични органи като НОИ, НАП и др., във връзка с изпълнение на своите законови изисквания. При поискване, лични данни могат да бъдат предоставяни и на други официални органи – МВР, Прокуратура и др., при получено по съответния ред запитване, съгласно **П 5-2**.
ИАСАС гарантира, че личните данни не се разкриват на неупълномощени трети страни, членове на семейството или приятели, включително на държавни или разследващи органи, ако има основателно съмнение, че не се изискват по установения ред.
Всеки служител, на когото бъде поискано разкриване на обработвани лични данни за друго лице от трета страна, трябва да прецени дали разкриването на информацията е свързано с нуждите на дейността, извършвана от организацията. ДЛЗД провежда периодични обучения на лицата, обработващи лични данни, с цел избягване на риска от неправомерно разкриване на лични данни на трети страни.

5.6. Трансграничен трансфер на лични данни
Към този момент ИАСАС не извършва трансфер на личните данни, които събира и обработва. При евентуална промяна в ситуацията, преди да се предадат лични данни извън Европейския съюз, трябва да бъдат приложени адекватни предпазни мерки, включително подписване на споразумение за прехвърляне на данни, и при необходимост трябва да бъде получено разрешение от Комисията за защита на личните данни. Дружеството, което получава

личните данни, трябва да спазва принципите за обработка на лични данни. Редът за осъществяване на предаването на данни е посочени в **П 5-8 Трансфер на лични данни**.

ГЛАВА 6. ПРИНЦИПИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Обработката на лични данни в ИАСАС се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите, разработени и прилагани в ИАСАС, гарантират спазването на тези принципи.

"Законосъобразност, добросъвестност и прозрачност" – данните са обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данни;

"Ограничение на целите" – данните са събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели;

"Свеждане на данните до минимум" – данните са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;

"Точност" – данните са точни и при необходимост се поддържат в актуален вид; предприемат се всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

"Ограничение на съхранението" – данните са съхранявани във форма, която позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни;

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

"Отчетност" – Администраторът е в състояние да докаже спазването на принципите, свързани с обработването на личните данни.

ГЛАВА 7. ОБЩИ НАСОКИ ЗА ОБРАБОТКА НА ЛИЧНИ ДАННИ

7.1. Законосъобразност на обработването

Всяко обработване на лични данни трябва да бъде законосъобразно и добросъвестно.
Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

- субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;
- обработването е необходимо за изпълнение на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- обработването е необходимо за спазването на законово задължение, приложимо за ИАСАС;
- обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данни или на друго физическо лице;
  обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на ИАСАС;

7.2. Цели на обработването

ИАСАС обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели, а именно:

- за изпълнение на дейностите по сортоизпитване, апробация и семеконтрол;
- управление на човешките ресурси;
- финансово-счетоводна дейност;
- пенсионна, здравна и социално осигурителна дейност;
- управление на собственост;
- други.

Личните данни трябва да се обработват само за целите, за които първоначално са били събрани. При необходимост събраните лични данни да бъдат обработвани за друга цел, субектът следва да бъде уведомен допълнително затова или трябва да му бъде поискано съгласието, в случай че не е налице друго основание за обработване на данните. За всяко такова искане във **Ф 5-0.1 Декларацията за съгласие** трябва да се посочи първоначалната цел, за която са събрани данните, новата или допълнителната(ите) цел(и), както и причината за промяна.

7.3. Получаване на съгласие

Когато обработването на лични данни, включително специални категории лични данни, се основава на съгласието на субекта на данните, ДЛЗД е отговорен за поддържането на доказателство (запис) за даденото съгласие и че то е:

- свободно изразено – дадено без натиск или заплаха от неблагоприятни последици;
- конкретно – дадено за конкретна цел и за определена категория лични данни;
- информирано – дадено на база получената чрез Политика за поверителност информация;
- недвусмислено – не се извлича или предполага от други изявления/декларации подписани от лицето;
- дадено с активно действие – чрез подписване на писмена декларация или онлайн, вкл. устно.

Не се допуска съгласието да бъде обвързано с предварителни условия или да води до неблагоприятни последици, в случай на отказ от съгласие или неговото оттегляне на по-късен етап.

ДЛЗД/Отговорното лице предоставя на субекта на данни **Ф 5-0.1 Декларация за съгласие**, при което го информира и гарантира, че неговото съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време, чрез попълване на **Ф 5-0.2 Декларация за оттегляне на съгласие.**

Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне.

Дейностите по обработка, основавани на съгласието се прекратяват, като за целта Длъжностното лице по защита на данните информира собственика на съответния процес за полученото оттегляне на съгласие.

Когато се събират лични данни на дете на възраст под 18 години, ДЛЗД/Отговорното лице изисква родителско съгласие преди събирането, като предоставя за подпис **Ф 5-0.3 Декларация за родителско съгласие,** при което информира родителя/настойника и гарантира, че неговото съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време, чрез попълване на **Ф 5-0.4 Декларация за оттегляне на родителско съгласие.**

Служител човешки ресурси поддържа **Ф 5-0.5 Регистър на получените/оттеглените съгласия**.

7.4. Обработване на специални категории лични данни

ИАСАС не обработва лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични и биометрични данни за целите единствено на идентифицирането на

физическо лице/, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.
Изключения се допускат, ако е налице едно от следните условия:

- субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели;
- обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на ИАСАС или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила;
- 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;
- обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;
- обработването е необходимо с цел установяване, упражняване или защита на правни претенции;
- обработването е необходимо по причини от важен обществен интерес, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи мерки за защита на основните права и интереси на субекта;
- 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;
- обработването е необходимо от съображение от обществен интерес в областта на общественото здраве;

7.5. Осигуряване на точност на данните

7.5.1. Данните, които се съхраняват от ИАСАС, се преглеждат редовно и актуализират при необходимост. Не се съхраняват данни, за които има съмнения в тяхната точност.

7.5.2. Длъжностното лице за защита на данните осигурява обучение на персонала относно изискванията за събирането на точни данни и тяхното поддържане.

7.5.3. Задължение на субекта на данни е да декларира, че данните, които представя на ИАСАС са точни и актуални.

7.5.4. От служителите, както и от клиентите/партньори и др. се изисква да уведомят своевременно ИАСАС за всякакви настъпили промени в данните, за да могат данните да бъдат актуализирани. Отговорният служител за съответната дейност регистрира всяко постъпило уведомление относно настъпила промяна (по реда на **П 5-2 Управление на искания от субекти на данни**) и гарантира, че ще бъдат предприети последващи действия за актуализиране на данните.

7.5.5. Минимум веднъж годишно Длъжностното лице по защита на данните преглежда събираните лични данни и сроковете за тяхното съхранение, като целта е да бъдат идентифицирани такива данни, които вече не се изискват за регистрираната цел. В случай, че бъдат открити такива данни, ДЛЗД предлага тяхното унищожаване, в съответствие с **П 5-3 Съхранение и запазване на лични данни**.

7.5.6. Отговорният служител, към които е насочено искането за корекция, отразява промяната в рамките на един месец, съгласно **П 5-2 Управление на искания от субекти на данни**. Този срок може да бъде удължен с не повече от два месеца за по-специфични заявки. Ако ИАСАС реши да не се съобрази с искането, след съгласуване с Длъжностното лице по защита на данни, началникът на съответния отдел изпраща отговор на субекта на данни, в който обяснява мотивите си и информира субекта за правото му да подаде жалба пред надзорния орган, както и да потърси правна защита.

7.5.7. Длъжностното лице по защита на данните информира третите страни, обработващи лични данни от името на ИАСАС, и препраща по подходящ начин коригираните лични данни.

7.6. Спазване на принципа на отчетност

ИАСАС доказва спазването на принципите за защита на данните като прилага настоящия Наръчник по защита на данните и документите, произлизащи от него, и в тази връзка внедрява и поддържа подходящи технически и организационни мерки за защита, въвежда мерки и техники за защита на данните на етапа на проектирането, извършва оценка на въздействието върху защитата на личните данни, уведомява надзорния орган при нарушение и др.

ГЛАВА 8. ПРАВА НА СУБЕКТА НА ДАННИ

8.1. Прозрачност, комуникация и условия за упражняване на правата на субекта

ИАСАС се ангажира и предоставя на субекта на лични данни всякаква информация съгласно чл. 13 и 14 на Регламента и всякаква комуникация по чл. 15-22 и чл. 34, която се отнася до обработването на данни в писмен или електронен вид в кратка, ясна и лесно достъпна форма. Допуска се информацията да бъде дадена устно, при условие, че самоличността на субекта е ясно доказана.

Правилата за осигуряване на прозрачност при обработването са регламентирани в **П 5-1 Прозрачност на обработването.**

8.2. Информация, предоставяна на субекта на данни

По време на или преди получаването на лични данни за всякакъв вид обработка, субектът има възможност да се запознае с **Ф 5-1.1 Политика за поверителност** поместена на сайта на ИАСАС, в която се съдържа информация за:

- данните, идентифициращи ИАСАС (администратора/обработващия), както и актуалните контактни данни, вкл. данните за връзка с Длъжностното лице по защита на данните;
- категориите (видовете) събирани лични данни, вкл. чувствителни лични данни, когато данните не са получени от субекта на данни;
- целите, за които се обработват личните данни, и правното основание, когато има такова;
- законните интереси, преследвани от ИАСАС или трета страна, когато обработването се извършва на основание чл. 6 параграф 1 е) от Регламента;
- методите на обработване;
- срока, за който се обработват личните данни;
- получателите или категориите получатели на личните данни, ако има такива;
- източника на данни, включително ако данните са от публично достъпен източник, когато данните не са получени от субекта на данни;
- намерението на ИАСАС да предаде личните данни на трета страна, когато е приложимо;
- съществуването на автоматизирано вземане на решения, включително профилирането, ако има такова;
- информация за всички права, които субектът на данни има;
- правото на жалба до надзорния орган;
- дали предоставянето на лични данни е нормативно или договорно изискване, дали субектът е задължен да предостави данните си и евентуалните негативни последствия, ако откаже да предостави данните си.

Когато ИАСАС възнамерява на по-късен етап да обработва личните данни за цел, различна от тази, за която първоначално са събрани, ДЛЗД информира субекта преди данните да бъдат обработени.
Редът за уведомяване на субекта на данни е регламентиран в **П 5-1 Прозрачност на обработването.**

8.3. Достъп от субектите на данни

ДЛЗД е отговорно да предостави на субектите на данни потвърждение дали се обработват техни лични данни и механизъм, който им позволява достъп до личните им данни и възможност да актуализират, коригират, изтриват, ограничават или пренасят своите лични данни. Механизмът за достъп е описан в **П 5-2 Управление на искания от субекта на данни.**

8.4. Коригиране и изтриване

Субектът на данни има право да поиска от ИАСАС да бъдат коригирани без забавяне личните му данни, които са неточни.
Субектът на данни има право да поиска от ИАСАС, а ДЛЗД осигурява изтриване на съхраняваните лични данни без забавяне, когато:

- личните данни повече не са необходими за целите, за които са били събрани;
- субектът оттегля своето съгласие и няма друго законно основание за обработването;
- субектът възразява срещу обработването съгласно чл. 21, параграф 1 или параграф 2 на Регламента и няма друго законно основание за обработването;
- личните данни са били обработвани незаконосъобразно.

Искането може да не бъде зачетено (на основание чл. 17, пар. 3, букви б) и д), в случай че обработването е необходимо във връзка с:

- установяването, упражняването или защитата на правни превенции;
- за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

ДЛЗД уведомява по подходящ начин другите администратори/обработващи лични данни на субекта за постъпилото искане.
Правото на изтриване не се прилага, доколкото обработването е необходимо за установяване, упражняване или защита на правни претенции.
Редът за изпълнение на исканията за коригиране и изтриване е описан в **П 5-2 Управление на искания от субекта на данни**.

8.5. Ограничаване на обработването

Субектът на данни има право да поиска от ИАСАС, а ДЛЗД е отговорен да ограничи обработването, както следва:

- когато точността на данните се оспорва от субекта на данни, обработването се ограничава за срока, необходим на ДЛЗД да извърши проверка на точността на данните;
- когато данните се обработват неправомерно, но субектът не иска изтриване, а само ограничаване на обработването;
- когато ИАСАС не се нуждае повече от личните данни за обработване, но субектът ги изисква във връзка с евентуални правни претенции;
- субектът на данните е възразил срещу обработването съгласно чл. 21, параграф 1 на Регламента, докато трае проверката на законните основания.

Когато обработването е ограничено, такива данни подлежат само на съхранение и тяхното обработване се допуска единствено със съгласието на субекта или за защита на правни претенции, или защита на правата на друго физическо лице.

ДЛЗД уведомява другите администратори/обработващи лични данни на субекта за постъпилото искане.
В случай на отмяна на ограничението, ДЛЗД своевременно уведомява субекта на личните данни.

8.6. Преносимост на данни
Субектите на данни имат право да получат при поискване копие от данните, които са предоставили на ИАСАС в структуриран и приложим за машинно четене формат и да предадат тези данни на друг администратор безплатно, в случаите, в които:

- обработването се основава на съгласие или на договорно задължение;
- данните се обработват по автоматизиран начин.

ДЛЗД осигурява, че тези искания се обработват в рамките на един месец, не са прекомерни и не засягат правата и свободите на други физически лица.
Когато е технически възможно, субектът може да поиска пряко прехвърляне на данните на другия администратор.
Механизмът за заявяване е описан в **П 5-2 Управление на искания от субекти на данни.**

8.7. Право на възражение
Субектът на данни има право да възрази срещу обработването на личните му данни, което се основава на необходимост от изпълнение на задача от обществен интерес, упражняване на официални правомощия, предоставени на администратора, съгласно чл. 6, параграф 1 буква д) от Регламента.
ДЛЗД осигурява, че това обработване ще бъде прекратено, освен ако не са на лице доказателства за убедителни законови основания, които имат предимство пред интересите, правата и свободите на субекта или за защита на правни претенции.

ГЛАВА 9. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Инвентаризацията на дейностите по обработка в ИАСАС се използва за регистриране и следене на обработваните от Агенцията лични данни, с което да се осигури единен подход към осигуряването на отчетност и спазване на изискванията на регламента.
Инвентаризацията помага на ИАСАС да разбере какви лични данни се обработват, както и какви политики и процедури за защита на данните да разработи. Освен това, в случай на проверка от надзорните органи, регистърът се използва, за да докаже, че Агенцията е осведомена и контролира дейностите си по обработване на данни.
Редът за изготвяне и поддържане на Регистър на дейностите по обработване на лични данни е описан в **П 5-5 Инвентаризация на личните данни.**

ГЛАВА 10. ТРАНСФЕР НА ДАННИ

ИАСАС не предава лични данни, които да се обработват или да са предназначени за обработване след предаване на трета държава (държави, които не са членки на Европейския съюз или част от Европейското икономическо пространство) или на международна организация.
В случай че ИАСАС започне да предава на трети държави (държави, които не са членки на Европейския съюз или част от Европейското икономическо пространство) или на международни организации лични данни за обработване, трябва да бъдат приложени адекватни предпазни мерки, включително подписване на споразумение за прехвърляне на данни, и при необходимост трябва да бъде получено разрешение от Комисията за защита на личните данни. Дружеството, което получава личните данни, трябва да спазва принципите за обработка на лични данни.

ГЛАВА 11. СИГУРНОСТ НА ОБРАБОТВАНЕТО

ИАСАС прилага подходящи технически и организационни мерки за защита, които са насочени към рисковете, свързани с обработването като неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или по друг начин обработвани лични данни.
При оценяването и избора на подходящи технически мерки за защита, Длъжностното лице по защита на данните съвместно с IT специалист вземат предвид:

- антивирусна защита;
- защита на мобилни компютри и устройства;
- защита с пароли;
- защита на електронна поща;
- защита на носители на информация;
- защита на мрежовите услуги;
- използване на криптографски механизми за контрол;
- технологии като псевдонимизиране и анонимизиране;
- възможността за възстановяване на наличността и достъпа до лични данни, в случай на възникнал физически или технически инцидент;
- възможността за внедряване на международни стандарти за сигурност, като ISO 27001 и др.

При оценяването и избора на подходящи организационни мерки за защита се взема предвид:

- възможността за непрекъснато обучение и повишаване на осъзнатостта на служителите по въпросите на сигурността на личните данни;
- гарантиране на сигурността и компетентността на персонала, работещ с лични данни;
- въвеждане и прилагане на дисциплинарен процес по отношение на правилата за защита на личните данни;
- прилагане на политика "чисто бюро, чист екран";
- права на достъп в системи/помещения;
- взаимоотношения с доставчици, гарантиращи сигурността на обработваните лични данни;
- въвеждане на процес на редовно изпитване и наблюдение на изпълнението, и последваща оценка на ефективността на прилаганите технически и организационни мерки, и др.

Всеки служител на ИАСАС, чиито отговорности включват обработване на лични данни, е отговорен и гарантира тяхната защита и това, че данните се съхраняват сигурно и не се разкриват при никакви обстоятелства на трети страни, освен ако няма официално възлагане за обработване по реда на **П 5-4 Взаимоотношения с доставчици**.

Личните данни се обработват в условия на максимална сигурност, както следва:

- данните, съхранявани на преносими носители, са защитени чрез мерките за контрол, описани в **СП 6-1 Използване на мобилни устройства и на сменяеми информационни носители**
- обработването на лични данни извън обекта на ИАСАС, което носи значителен риск от увреждане/изтичане, се извършва в съответствие с **СП 6-2 Работа от разстояние**;
- с цел предотвратяване на изтичане и загуба на информация е въведена класификация на информацията по степен на чувствителност, съгласно **СП 6-9 Класификация на информацията**;
- достъпът до вътрешните системи и ресурси се управлява, като предоставените права за достъп са в съответствие с делегираните правомощия и изпълнявани отговорности, съгласно **СП 6-4 Управление на достъпите и автентикацията;**
- данните на хартиен носител се съхраняват в помещения с контролиран достъп и/или в заключващи се шкафове; достъпът до офисите и помещенията се извършва по реда на **СП 6-6 Физическа сигурност на информационните активи;**
- паролите са общо използван тип тайна информация за автентификация и са средство за верифициране на идентичността на потребителя. Редът за управление на паролите е описан в **СП 6-7 Генериране и съхранение на паролите**;
- в зависимост от чувствителността на данните и оценения въздействие върху тяхната сигурност, може да се използват различни техники за допълнителна защита по реда на **СП 6-3 Използване на криптографски механизми**;
- не се допуска документи на хартиен носител да се изнасят от определените за целта помещения без изрично разрешение от ДЛЗД, както и да бъдат оставяни на места, на които ще бъдат достъпни до неоторизирани лица, като за целта се спазва реда на **СП 6-1 Използване на мобилни устройства и на сменяеми информационни носители**;
- данните, обработвани в електронна среда (като файлове) или обработвани в софтуерни системи са защитени посредством механизми, разписани в **СП 6-4 Управление на достъпите и автентикацията**, **СП 6-7 Генериране и съхранение на паролите**;
- с цел предпазване на данните от случайно изтриване е приложена политика по резервиране на тези данни, по реда на **П 6-7 Създаване на резервни копия на информацията, информационните и комуникационни системи;**
- личните данни могат да бъдат изтривани или унищожавани само в съответствие с заложените срокове в системата. Документите на хартиен носител, чийто срок на съхранение е изтекъл се унищожават чрез шредиране, преди да бъдат третирани като отпадък. Данните върху твърдите дискове на излезли от употреба персонални компютри трябва да бъдат изтрити или дисковете унищожени;
- системите и процесите също трябва да бъдат редовно тествани за уязвимости.
- сигурността на информацията, обменяна по електронен път вътре в организацията или с външни обекти, както и безопасното използване на интернет ресурси е описана в **СП 6-8 Допустимо използване на ИКС, електронна поща, интернет**;
- въведена е практика за регистриране в лог файлове в информационните системи – събития, записващи дейности на потребители, изключителни случаи, грешки и събития и т.н., съгласно **СП 6-12 Съхранение на записи за събития (логове) на информационните системи.**

Всеки служител, обработващ лични данни, преминава през начално и периодично обучение по изискванията на Регламента и подписва декларация, с която приема да спазва въведените организационни и технически мерки за осигуряване на защита на личните данни в ИАСАС.

ГЛАВА 12. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

В случаите, в които извършените операции по обработване са включени в оповестения списък от надзорния орган в страната, или по решение на ръководството на ИАСАС, се извършва оценка на въздействието върху защитата на данните за всяка дейност по обработка на данни съгласно **П 5-7 Оценка на въздействието върху защитата на данните**.
При оценката се разглеждат тежестта и вероятността от нарушаване на сигурността, което може да доведе до евентуална вреда или загуба на правата и свободите на субекта на лични данни, както и до евентуални влияния върху репутацията и доверието в ИАСАС.

ГЛАВА 13. УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ. УВЕДОМЯВАНЕ ЗА НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Когато ИАСАС установи, че е налице предполагаемо или действително нарушение в сигурността на личните данни, ДЛЗД трябва да извърши вътрешно разследване и своевременно да предприеме подходящи мерки за отстраняване, в съответствие с **П 5-6 Управление на инциденти с лични данни. Уведомяване при нарушаване на сигурността на данните**.
Когато съществува риск за правата и свободите на субектите на данни, ИАСАС трябва да уведоми съответните органи за защита на данните без неоснователно забавяне и, когато е възможно, в рамките на 72 часа.

ГЛАВА 14. УПРАВЛЕНИЕ НА НАЛИЧНОСТТА И ПЛАН ЗА ВЪЗСТАНОВЯВАНЕ

ИАСАС създава, поддържа и периодично изпитва **План за възстановяване,** който определя реда и отговорностите в ИАСАС за възстановяване на ИТ инфраструктура, ИТ услуги и всички данни, включително лични данни в определени срокове, в случай на възникнало бедствие или друг разрушителен инцидент.
Целта на този план е да гарантира възстановяването на ИТ инфраструктура, ИТ услуги и данни в рамките на зададеното целево време за възстановяване (RTO).
Този план включва всички ресурси и процеси, необходими за възстановяване, и обхваща всички аспекти на сигурността на данните в управлението на непрекъснатостта на бизнеса.

План за възстановяване се съхранява по следния начин:

- планът трябва да бъде поддържан и на хартия, така че в случай на отпадане на електрическо захранване, сървър или друго, да бъде наличен на местата за ползване;
- копия на документа трябва да се поддържат от минимум двама от членовете на екипа извън сградата на ИАСАС (напр. вкъщи);
- електронната форма на документа се съхранява на сървъра на ИАСАС.

ДЛЗД/Друг служител (Системен администратор) организира ежегодни симулации на плана, за да установи неговата ефективност и готовността на персонала за реакции, като поддържа записи за резултатите.
ДЛЗД/Друг служител проверява и при необходимост актуализира документа най-малко веднъж годишно.
При оценката на ефективността и адекватността на плана се вземат под внимание следните критерии:

- резултатите от проведени упражнения;
- в случай на симулация/реална криза дали възстановяването е приключило в рамките на целевото време за възстановяване.

ГЛАВА 15. ОБУЧЕНИЕ НА ПЕРСОНАЛА

Висшето ръководство на ИАСАС осигурява осведомеността и осъзнаването на служителите, относно необходимостта от съответствие с изискванията на Регламент (ЕС) 2016/679, като организира въвеждащи поддържащи обучения за запознаване с установените политики и процедури и свързаните с тях задължения на всеки служител на ИАСАС.
Длъжностното лице по защита на данните гарантира, че всички служители, чиято дейност е свързана с обработване на лични данни или имат постоянен/редовен достъп до лични данни, са преминали съответните обучения и познават, и прилагат изискванията за защита на личните данни.
Длъжностното лице по защита на данните изготвя **Ф 2-1.2 Годишна програма за обучение**, която включва както обучения за целия личен състав, така и за всяка конкретна позиция, която има отношение към обработването на лични данни.
Датата на всяко проведено обучение се отразява в предвиденото за целта място във **Ф 2-1.2 Годишна програма за обучение** и във **Ф 2-1.3 Протокол от вътрешно обучение.**
Длъжностното лице по защита на данните поддържа списък/протокол с имената и подписите на присъствалите на съответните обучения.

ГЛАВА 16. МОНИТОРИНГ, ИЗПИТВАНЕ И ОЦЕНКА НА ЕФЕКТИВНОСТТА

16.1. Общи положения

Настоящата глава регламентира реда и отговорностите на персонала на ИАСАС за осъществяване на дейностите по мониторинг, изпитване, анализ и оценяване, необходими за осигуряване на съответствие на дейностите по обработване на лични данни с изискванията на Регламента.
В ИАСАС се извършва периодично наблюдение, измерване, анализ и оценяване, на базата на определени показатели.

16.2. Дефиниране на параметрите, подлежащи на мониторинг и изпитване

Длъжностното лице по защита на данните обобщава процесите и мерките за контрол, свързани със защитата на личните данни, които подлежат на наблюдение и измерване и изготвя **Ф 4-1.1 План за наблюдение и измерване**, който се утвърждава от Изпълнителния директор.
Определянето на обектите и дейностите по наблюдение и измерване е резултат от извършеното преценяване на риска и оценката на въздействието.
За осигуряване на валидни резултати за целите на анализа и оценяването, ДЛЗД определя методите за наблюдение и измерване, които документира във **Ф 4-1.1 План за наблюдение и измерване**.

Ф 4-1.1 План за наблюдение и измерване се преразглежда минимум веднъж годишно от ДЛЗД и при необходимост се актуализира.

Резултатите от мониторинга и изпитването се отразяват от ДЛЗД във **Ф 4-1.2 Контролен лист** или в документ от външна организация, наета да извършва наблюдение.

16.3. Анализ на данните и оценяване на резултатите

Данните, събрани при наблюдението и измерването, се обобщават, анализират и оценяват при периодичност, определена във **Ф 4-1.1 План за наблюдение и измерване**.
Получените при анализа резултати се използват от ДЛЗД за оценяване на:

- ефективността на внедреното планиране и мерки за контрол;
- ефективността на предприетите действия за овладяване на рисковете;
- необходимостта от подобряване на защитата на личните данни.

Веднъж годишно, ДЛЗД измерва и оценява ефективността на избраните механизми за контрол или групи механизми за контрол и прави запис във **Ф 4-1.3 Измерване и оценка на**

ефикасността. Целта е да се потвърди дали са изпълнени изискванията за резултатност по отношение на защитата на личните данни.
При необходимост, вследствие на извършеното наблюдение и контрол, се актуализира **Ф 4-1.1 План за наблюдение и измерване** и/или оценените рискове и въздействия.