Утвърждавам: ....
доц. Ива Угринова - директор на ИМБ - БАН

ВЪТРЕШНА ИНСТРУКЦИЯ ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ВИНСТИТУТ ПО МОЛЕКУЛЯРНА БИОЛОГИЯ ПРИ БАН

Раздел първи ПРАВНА РАМКА

Чл. 1. Настоящата Инструкция е изготвена в съответствие с разпоредбите на:

1. Регламент N°2016/679 (ЕС) на Европейския парламент и на Съвета от 27.04.2016 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 (ОРЗД));

2. Насоки от Работна група по чл. 29 с оглед на началото на прилагането на Общия регламент за защита на данните.

Раздел втори ДЕФИНИЦИИ

Чл. 2. За целите на Инструкцията, понятията по-долу имат следното значение:

1) *„лични данни”* означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

2) *„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;

3) *„ограничаване на обработването*" означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4) *„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;

5) *„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;

6) *„обработващ лични данни"* означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

7) *„получател"* означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

8) *„трета страна"* означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

9) *„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;

10) *„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;

11) *„генетични данни"* означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по- специално, от анализ на биологична проба от въпросното физическо лице;

12) *„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;

13) *„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;

14) *„надзорен орган"* означава независим публичен орган, създаден от държава членка действащ на основание GDPR или друго приложимо законодателство, а в конкретния случай - Комисия за защита на личните данни с адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2, уебсайт: https://www.cpdp.bg.

Раздел трети ЦЕЛИ И ОБХВАТ. ПРИНЦИПИ

Чл. 3. Инструкцията има за цел:

1. Установяване на ясни правила и контрол при събиране, обработване, съхраняване и трансфер на лични данни от Институт по молекулярна биология при БАН (ИМБ- БАН), наричано по-нататък за краткост „Администраторът".

2. Определяне на необходимите технически и организационни мерки за защита на личните данни от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до предадени, съхранявани и/или обработени по друг начин лични данни, което би могло да доведе до физически, материални п/или нематериални вреди.

3. Разписване на ясни процедури за действие в случай на нарушаване на сигурността на данните, събирани, обработвани и съхранявани от Администратора.

4. Регламентиране задълженията на обработващите лични данни лица и/или лицата, които имат достъп до такива данни и работят под ръководството на обработващите лични данни, в случай на нарушение на сигурността на данните.

Чл. 4. При обработването на лични данни, Администраторът спазва следните принципи и условия за тяхната имплементация:

1. Данните се обработват законосъобразно и по прозрачен начин, като се гарантира добросъвестност по отношение на субектите на данни *(„законосъобразност, добросъвестност и прозрачност* "), а именно:

1.1. Принципът на законосъобразност, по смисъла на чл. 6, § 1, буква в) от Регламента е спазен доколкото в определени случаи обработването е необходимо за спазване на законово задължение за администратора да събира, съхранява и обработва лични данни на служителите, с оглед изпълнението на трудовото правоотношение и нормативно установените задължения, които произтичат в тази връзка, или обработването е необходимо на основание чл. 6, § 1, буква б) от Регламента, с оглед изпълнението на различни договори за услуги (граждански, посреднически и др.), т.е. обработването на данните е необходимо за изпълнението на договор, по който субектът на данните е страна.

1.2. Принципът на добросъвестност е приложен доколкото обработването е необходимо „за" и пропорционално „на" целите и задачите, стоящи пред него и същото не излиза и не надхвърля съответните цели и задачи;

j 1.3. Принципът на прозрачност се изразява в обема от информация, която се предоставя от страна на администратора, от начина и средствата за комуникация със субектите на данни в процеса на обработването.

2. Данните се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели (*„ограничение на целите").*

3. Събираните данни са подходящи, свързани със и ограничени до необходимата информация във връзка с целите, за които се обработват (*„свеждане на данните до минимум").*

4. Данните са точни и актуални,, като се имат предвид целите, за които те се обработват *(„точност").*

5. Данните са съхранявани във форма, която, позволява идентифицирането на субекта на данни за период, не по-дълъг от необходимия за целите на обработването им *(„ограничение на съхранението").*

6. Данните са обработвани по начин, който гарантира подходящо ниво на сигурност,

«

включително защита срещу неразрешено или незаконосъобразно обработване и случайна загуба, унищожение или повреждане, като се прилага подходяща технология *(„цялостност и поверителност").* ,

7. Администраторът спазва принципа за забрана на обработване на специални категории данни, очертани в чл. 9 от Регламента, в това число: данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, 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, като изключения се допускат само в случаите, предвидени в чл. 9, т. 2 от Регламента.

Чл. 5. Обработването на личните данни се извършва с цел:

(1) Индивидуализиране на трудовите и граждански правоотношения:

- изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, ДОПК и др.

- използване на събраните данни за съответните лица за служебни цели;

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения - за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

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

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

(2) Обработването е необходимо и при сключване и изпълнение на договори с клиенти и контрагенти с цел индивидуализиране на физическите лица и физическите лица представляващи юридическите лица.

Раздел четвърти ПРОЗРАЧНОСТ НА ИНФОРМАЦИЯТА. ПРАВА НА СУБЕКТИТЕ НА ДАННИ.

Чл. 6. Всички лица, чиито лични данни се обработват от ИМБ-БАН, имат права, гарантирани от Общия Регламент за защита на личните данни и Администраторът е задължен да осигури спазването им.

Чл. 7. (1) При събиране на лични данни от субекта на данните, администраторът предприема необходимите мерки за предоставяне на всякаква информация, която се отнася до обработването в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Информацията може да бъде дадена и устно при постъпило такова искане от страна на субекта на данните при условие, че идентичността му е доказана с други средства.

(2) Своевременно след получаване на личните данни от субекта на данните, администраторът му предоставя информация за:

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

б) когато е приложимо - координатите за връзка с длъжностното лице по защита на данните;

в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

г) когато обработването се извършва въз основа на член 6, параграф 1, буква е) от Регламента, законните интереси, преследвани от администратора или от трета страна;

д) получателите или категориите получатели на личните данни, ако има такива;

е) когато е приложимо - намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита.

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

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

и) когато обработването се основава на член 6, параграф 1, буква а) или член 9, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

й) правото на жалба до надзорен орган;

к) дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

л) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4 от Регламента, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

(3) На субекта на данни е осигурена информация и за това, че предоставянето на данните съставлява нормативно изискване по смисъла на Кодекса на труда (по отношение на служителите), или е необходимо за сключване и изпълнение на договор (по отношение на клиентите); информация относно задължението на субектът за предоставяне на данните, както и какви биха били евентуалните последици при непредоставяне на съответните данни.

Чл. 8. (1) Администраторът предоставя информацията на субектите на данни в следните срокове:

а) в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;

б) ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или

в) ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

(2) В случай, че администраторът .възнамерява да обработва личните данни по- нататък за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация.

(3) Не се предоставя такава информация, когато и доколкото:

а) субектът на данните вече разполага с информацията;

б) предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия; по-специално за обработване на данни за целите на архивирането в обществен интерес, за .научни или исторически изследвания или за статистически цели, при спазване на условията и гаранциите по член 89, параграф 1 от Регламента, или доколкото съществува вероятност задължението да направи невъзможно или сериозно да затрудни постигането на целите на това обработване. В тези случаи администраторът взема подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните, което включва и предоставяне на публичен достъп до информацията;

в) получаването или разкриването е изрично разрешено от правото на ЕС или националното право, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на легитимните интереси на субекта на данните; или

г) личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, което се урежда от правото на Съюза или право на държава членка, включително законово задължение за поверителност.

Чл. 9. Във връзка с обработването на личните му данни, субектът на данни разполага със следните права:

1) Право на достъп - Всяко физическо лице има право на достъп до събраните лични данни, които го засягат и възможността да упражнява това право безплатно, лесно и на разумни интервали - всеки субект на данни има правото да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация относно целите, за които се обработват личните данни, категориите лични данни, които се събират, когато е възможно — срока, за който се обработват личните данни, получателите на личните данни, логиката на автоматизираното обработване на личните данни и последствията от такова обработване, най-малкото когато се извършва на основата на профилиране.

а./ Когато е възможно, администраторът предоставя на субекта на данните пряк достъп (достъп от разстояние) до системата, в която се съхраняват неговите лични данни, стига това право да не влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера.

б./ Когато обработваното количество информация относно субекта на данни е голямо, преди да бъде предадена информацията, администраторът може да поиска от субекта на данните, да посочи точно информацията или дейностите по обработването, за които се отнася искането.

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

г./ Когато исканията на субекта на данните са явно неоснователни или прекомерни и често повтарящи се, администраторът, след като докаже наличието на неоснователния или прекомерен характер на искането може да наложи разумна такса, като вземе предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или да откаже да предприеме действия по искането.

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

3) Право на изтриване (право „да бъдеш забравен") - Субектът на данните има право на коригиране на личните данни, свързани с него, както и правото „да бъде забравен", когато запазването на тези данни е в нарушение на Общия регламент или на националното право. По-специално, субектът на данни има право личните му данни да се изтриват и да не бъдат обработвани повече, когато престанат да бъдат необходими с оглед на целите, за които те са били събрани или обработвани по друг начин, когато субектът на данните е оттеглил своето съгласие или е възразил срещу обработването на лични данни, свързани с него.

4) Право на ограничаване на обработването - Субектът на данните има право да изиска от администратора ограничаване на обработването, когато се прилага едно от следното:

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

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

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

г) субектът на данните е възразил срещу обработването съгласно член 21, параграф 1 от Регламента в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

Когато субект на данните е изискал ограничаване на обработването, администраторът го информира преди отмяната на ограничаването на обработването.

5) Право на преносимост на данните - Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато:

а) обработването е основано на съгласие в съответствие с член 6, параграф 1, буква а) или член 9, параграф 2, буква а) или на договорно задължение съгласно член 6, параграф 1, буква б) от Регламента, и

6) обработването се извършва по автоматизиран начин.

Когато упражнява правото си на преносимост на данните, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо. Упражняването на правото не засяга правото на изтриване и не влияе неблагоприятно върху правата и свободите на други лица.

б) Право на възражение - Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на член 6, параграф 1, буква д) или буква е) от Регламента, включително профилиране, основаващо се на посочените разпоредби. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни, отнасящо се до нето за този вид маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг. Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява. Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото му, което му се представя по ясен начин и отделно от всяка друга информация.

7) Права при автоматизирано вземане на индивидуални решения, включително профилиране - Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен. Това не се прилага, ако решението:

а) е необходимо за сключването или изпълнението на договор между субект на данни и администратор;

б) е разрешено от правото на ЕС или националното право, което се прилага спрямо администратора, и в което се предвиждат също подходящи мерки за защита на правата и свободите, и легитимните интереси на субекта на данните; или

в) се основава на изричното съгласие на субекта на данни.

В случаите, посочени в букви а) и в), администраторът прилага подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните, най-малко

правото на човешка намеса от страна на администратора, правото да изрази гледната си точка и да оспори решението.

Чл. 10. (1) Субектите 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 Общия регламент и националното законодателство.

(2) Данните за контакт с длъжностното лице по защита на данните може да се публикуват на интернет страницата на Администратора и се съобщават на всички служители, както и на Комисията за защита на личните данни.

Раздел пети
ОБХВАТ, ФОРМА И СРОК ЗА СЪХРАНЕНИЕ НА ДАННИТЕ.

Чл. 11. (1) Данните, които се събират и обработват при изпълнение на нормативно установеното задължение на администратора като страна по трудовото правоотношение, и/или в изпълнение на сключен договор със субекта на данни, са сведени до необходимия минимум във връзка с целите, за които се обработват.

(2) За служителите в общия случай се обработват следните данни: три имена; единен граждански номер /ЕГН/; данни от лична карта; точен адрес; банкова сметка; телефон и e- mail; данни за здравословното състояние; притежавано образование и професионална квалификация; име и ЕГН на деца и съпруг/а, когато служителят желае да ползва данъчни облекчения и е необходимо попълване на декларации и др. документи по чл. 22в и сл. от ЗДДФ/1. За определени длъжности е допустимо разширяване обхвата на събираните лични данни, в това число свидетелство за съдимост за лица, заемащи материалноотговорни длъжности, по смисъла на Закона за счетоводството, Закона на частната охранителна дейност и прочие, удостоверение за психологическа годност и свидетелство за управление на МПС за длъжността шофьор, изискуеми съгласно Закона за движение по пътищата и други.

(3) По отношение на лицата, с които са сключени граждански договори се обработват следните данни: три имена; единен граждански номер /ЕГН/; данни от лична карта; точен адрес; банкова сметка; телефон и e-mail.

Чл. 12. Обработване на данни може да се извършва и посредством запис чрез технически средства за видеонаблюдение, за целите на предотвратяването на измами, с оглед гарантиране сигурността на помещенията, в които се извършва дейността на администратора, включително сигурността на субектите на данни, контрол на работния процес и спазване на работното време, опазване имуществото на администратора от противоправни посегателства, както и тяхното предотвратяване и пресичане. В тези случаи администраторът ще предприеме действия по информираност на субектите на данни чрез поставяне на обозначителни табели, указващи че обектът се намира под постоянно видеонаблюдение.

Чл. 13. (1) Личните данни се предоставят от субектите на данни и се обработват след предоставяне на информация на лицата за техните права съгласно Общия регламент.

(2) Обработването на извършва след предоставяне на изрично и доброволно съгласие от страна на субектите на данните, дадено свободно, конкретно, информирано и недвусмислено.

Чл. 14.(1) Личните данни в досието на служителите и информацията, съдържаща се във ведомостите за заплати ще бъдат съхранявани 50 години. Информацията, свързана с финансовите условия по договорите (за целите на счетоводните регистри, финансовите отчети и последващи финансови инспекции) се съхранява до 10 години след отчетния период за който се отнася.

(2) След изтичане на нормативно определения срок за съхранение, документите на хартиен носител, които съдържат лични данни на субектите на данни се унищожават физически, чрез машинно нарязване в присъствието на комисия от двама служители, определени от администратора или от външна фирма, наета за целта, а тези в електронен формат се изтриват.

(3) След нормативно определения срок за съхранение на данните, същите могат да бъдат запазени само ако са анонимизирани и субекта на данни не може да бъде идентифициран п/или с изричното му съгласие с посочване на конкретната цел, за която се иска продължаване на съхранението.

Чл. 15. При прекратяване дейността на Института без правоприемство, ведомостите за заплати се предават в Националния осигурителен институт по реда на чл. 5, ал. 10 от Кодекса за социално осигуряване.

Чл. 16. При прекратяване на трудово, служебно или облигационно правоотношение с обработващ лични данни, данните се предават на друго определено от администратора лице в присъствието на комисия.

Раздел шести ДОСТЪП ДО ЛИЧНИТЕ ДАННИ

Чл. 17. (1) Личните данни, обхванати от Инструкцията се предоставят в структурата на администратора на лицата със статут на обработващи лични данни.

(2) Всички служители на **ИМБ-БАН** при встъпване в длъжност се задължават да спазват конфиденциалност и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на трудовите / договорните им задължения.

(3) Служители, които имат достъп до и право да обработват лични данни, се определят със заповед на Администратора.

Чл. 18. (1) Събраните от ИМБ-БАН лични данни се предоставят на държавни органи и институции, във връзка с изпълнение на негови законоустановени функции и на тези органи и институции по Кодекса на труда, Кодекса за социално осигуряване, Закона за здравното осигуряване, Закона за облагане доходите на физическите лица, Закона за здравословни и безопасни условия на труд и в други законоустановени случаи.

(2) ИМБ-БАН предоставя данни при искане/разпореждане от страна на органите на досъдебното производство, разследващите органи, съдебните органи и тези на полицията, частните или държавни съдебни изпълнители, при спазване на реда и условията за това, съгласно законодателството на Република България.

Раздел седми
ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ ОТ ИМЕТО НА АДМИНИСТРАТОРА

Чл. 19. Обработването на личните данни, предмет на Инструкцията, може да бъде възложено на обработващи лични данни, които от името на администратора и в съответствие с неговите инструкции, изискванията на приложимото законодателство и с оглед защита на правата на субектите на данни, осъществяват всички дейности в този смисъл.

Чл. 20. (1) Обработващият лични данни следва да предприеме всички разумни стъпки, за да гарантира надеждност и конфиденциалност при обработване на данните и да предприеме необходимите мерки за ограничаване достъпът на други лица до тези данни.

(2) Обработващият лични данни декларира и гарантира навременното и пълно изпълнение на задълженията и отговорностите си по обработване на данните, в съответствие с приложимото законодателство.

(3) Обработващият лични данни се задължава да съхранява записи от всички извършени дейности по обработка на личните данни, като осигури всяка стъпка от обработването на данни да може да се проследи, включително на кои са предоставени данните, кога, какви данни, за каква цел и какви са договорките на обработващия с такива трети страни.

(4) Обработващият лични данни се задължава да обработва своевременно и правилно всички запитвания, свързани с обработката на лични данни, да съдейства на администратора за упражняване правата на субектите на лични данни и да изпълнява насоките на надзорните органи във връзка с обработване на прехвърляните данни.

Чл. 21. (1) Обработващите лични данни нямат право да разкриват личните данни на трети лица, освен ако не са упълномощени от администратора или това се изисква от приложимото законодателство.

(2) Ако държавен или надзорен орган изиска достъп до лични данни на администратора, обработващият следва да уведоми администратора преди разкриването, освен ако това не е забранено от закон.

Чл. 22. (1) Обработващият лични данни не включва друг обработващ данни без предварителното конкретно или общо изрично писмено одобрение от администратора.

(2) Обработващият лични данни уведомява предварително администратора за всяка планирана промяна за включване или замяна на други лица, обработващи данни като даде възможност на администратора да оспори тези промени.

(3) В случаите, когато обработващият лични данни включва друг обработващ лични данни за извършване на специфични дейности по обработване от името на администратора, по отношение на това лице се налагат същите задължения за защита на данните, както, задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни.

(4) Първоначалният обработващ лични данни носи пълна отговорност пред администратора за изпълнението на задълженията на другия обработващ лични данни.

Чл. 23. (1) Като се има предвид естеството на обработването, обработващият подпомага администратора за изпълнение на задълженията му по отношение на постъпили искания от страна на субектите на данни, съгласно приложимото за конодателство.

(2) Обработващият е длъжен незабавно да уведоми администратора, ако получи искане от субект на данни, както и да отговори на подобни искания по начин, определен от администраторът, освен ако е изискуемо от приложимото законодателство. В този случай, обработващият, доколкото това е позволено от приложимото законодателство, информира администратора относно тези изисквания, преди да отговори.

Чл. 24. (1) Обработващият следва в срок не по-късно от 24 часа да уведоми администратора, ако узнае за нарушение на сигурността на лични данни, предоставяйки на администратора достатъчно информация, която да му позволи да изпълни задълженията си да докладва на надзорния орган, а в определени случаи да информира субектите на данни за нарушението

(2) Уведомлението до администратора трябва да има най-малко следното съдържание:

а/ *Да* описва естеството на нарушението, категориите и броя на засегнатите субекти на данни, както и категориите и броя на засегнатите типове лични данни;

б/ *Да* съдържа имената и контактите на длъжностното лице за защита на данните на обработващия *(ако има такова лице)* и/или всеки друг контакт на лице, от което може да бъде получена допълнителна информация;

в/ Да описва вероятните последствия от нарушението на сигурността;

г/ *Да* описва мерките, които са взети или е предложено да бъдат взети срещу нарушението на сигурността на личните данни.

Чл. 25. (1) Обработващият лични данни следва да заличи или върне всички лични данни на администратора след приключване на услугите по обработване или по-рано, по изрично искане на администратора, освен ако няма нормативно установено изискване за тяхното съхранение.

(2) Обработващият лични данни осигурява достъп на администратора до цялата информация, необходима за доказване изпълнението на задълженията по обработването и съдейства за извършването на одити и проверки от страна на администратора или друг одитор, оправомощен от администратора.

Чл. 26. Обработващият следва да води регистър на дейностите по обработването, извършвано от името на администратора, в съответствие с разпоредбите на Общия регламент.

Чл. 27. Отношенията между администратора и обработващия данни се уреждат с допълнително споразумение към трудов/граждански договор.

Чл. 28. Администраторът определя със Заповед списък на лицата, които обработват лични данни в ИМБ-БАН.

Раздел осми
РЕГИСТРИ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Чл. 29. (1) За дейностите по обработване на лични данни, администраторът поддържа съответните регистри, съдържащи следната информация:

а/ името и координатите за връзка на администратора и — когато това е приложимо — на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните;

б/ името и координатите за връзка на обработващия или обработващите лични данни и — когато това е приложимо — на представителя на обработващия лични данни и на обработващите подизпълнители, ако има такива; в/ целите на обработването;

г/ описание на категориите субекти на данни и на категориите лични данни; д/ категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

е/ когато е възможно, предвидените срокове за изтриване на различните категории данни;

ж/ когато е възможно, общо описание на техническите и организационни мерки за сигурност, съобразени с нивото на риск.

(2) Регистрите могат да се поддържат в писмена форма, включително в електронен формат.

(3) При поискване, администраторът или обработващият лични данни и — когато това е приложимо — представителят на администратора или на обработващия личните данни, осигуряват достъп до регистъра на надзорния орган.

Чл. 30. Администраторът поддържа следния регистър:

а/ *Регистър "Персонал"* - в него се събират, обработват и съхраняват лични данни на служителите - физически лица, заети по трудови правоотношения;

Чл. 31. (1) В регистър „Персонал" се съхраняват следните видове лични данни:

1. Физическа идентичност - имена, ЕГН, адрес, телефон, данни по документ за самоличност (номер, дата на издаване и орган);

2. Образование - документ за придобито образование, специалност, място на придобиване на образованието, номер на диплома и дата на издаване, квалификация, правоспособност;

3. Трудова дейност - документи за трудов стаж и професионална биография;

4. Основание за обработката на специални категории данни по чл. 9 от Общия регламент и медицински данни - карта за предварителен медицински преглед за постъпване на работа и медицински документ за трудоустрояване (в случай, че субекти на данни с намалена трудоспособност са заети по трудов или граждански договор);

5. Свидетелство за съдимост, когато се изисква (напр. за материалноотговорни длъжности, служба по охрана).

6. Формуляр по образец и други данни в зависимост от законовите изисквания за конкретно заеманата длъжност, напр. свидетелство за управление на МПС/ данни от свидетелство за управление на МПС (номер, дата на издаване и орган).

7. Права на субектите - Отправени искания и запитвания от субекти на данни.

8. Нарушения на сигурността на данните - описание на констатирани случаи на пробив в сигурността на данните и предприетите действия и мерки от администратора.

9. Данни за контакт с длъжностното лице по защита на данните *(ако има такова).*

10. Предаване на трети лица и в трети страни, име и контакт с обработващия данните.

11 .Срок за съхранение.

(2) Данните в регистър „Персонал" се събират на хартиен и/ или технически носител и се обработвани съхраняват в отдел „Човешки ресурси".

(3) Данни за здравословното състояние на съответното лице се обработват във връзка с нормативно установеното изискване за изготвяне на здравни досиета на служителите от СТМ, както и във връзка с издаването на болнични листове (относно изплащане на обезщетения за временна неработоспособност, майчинство, за отглеждане на дете до две години и др.), а въз основа на решенията на ТЕЛК и НЕ/ІК, ИМБ-БАН, като работодател, издава производствени характеристики.

(4) Личните данни в регистър "Персонал" се набират при извършване на подбор за наемане на служители, при подаване на документи за постъпване на работа по трудово правоотношение и при подписване на трудови договори.

(5) При извършване на подбор за назначаване на служители, всеки кандидат подписва Декларация за съгласие за предоставяне на данни при подбор на персонал по образец, с която декларира, че доброволно е предоставил свои лични данни, посочени в професионалната си автобиография (вкл. трите си имена, ЕГН, придобито образование и опит, данни за контакт, други данни в зависимост от длъжността, за която се кандидатства) и/или други документи. Обработване на тези лични данни е само и единствено за целите на подбор и назначаване на персонал.

(6) Личните данни в регистър "Персонал" се съхраняват за следните срокове:

- при трудов договор - личните досиета на служителите и ведомостите за заплати ще бъдат съхранява 50 години;

- при граждански договор - за срока на действие на съответния Граждански договор и до 5 (пет) години след неговото прекратяване, като информацията, свързана с финансовите условия по Договора (за целите на счетоводните регистри, финансовите отчети и последващи финансови инспекции) ще бъде съхранявана 10 години след отчетния период, за който се отнася.

- Личните данни, събрани по реда на ал. 5 се съхраняват за срока на действие на процедурата по подбор на персонал и до 6 месеца след приключване на процедурата по прдбор на персонал, до изтичане на срока на изпитване на назначеното лице с оглед възможността да бъде поканен друг кандидат да заеме неговото място. При наличие на основание за това, периодът на съхранение на данните може да бъде по-дълъг, за което субектите на данни следва да бъдат своевременно уведомени.

„Персонал" имат следните права и задължения:

1. да използват личните данни при спазване разпоредбите на Кодекса на труда и другите нормативни актове, имащи отношения към трудовите правоотношения;

2. да не изнасят и съхраняват личните данни извън специално определените за целта места, регламентирани с режим на специален достъп;

3. да не използват личните данни по нерегламентиран начин /фалшифициране и друг вид злоупотреба/.

(2) С оглед осигуряване правата на служителите по трудов договор при пенсиониране, предвид задължението на Администратора, като работодател, по чл. 5, ал. 7 от Кодекса за социално осигуряване и предвид празноти в електронната система в съответните държавни институции за обработка и съхранение на данните относно осигурителния стаж и осигурителния доход на съответно лице, Администраторът съхранява данни за минал период на всички свои стари служители в Дружеството. Копия от тези документи и/или информация се предоставят само на съответния служител при направено лично искане от негова страна.

Чл. 33. (1) Защитата на помещенията, в които се съхраняват регистрите с личните данни се постига със заключване с ключ, като в самите помещения документите се съхраняват в шкафове, които също се заключват.

(2) Физическата защита на личните данни се осъществява от денонощна физическа охрана на сградата на Института.

(3) Данните от регистъра не се предават на трети лица без наличие на правно основание за това.

(4) Длъжностното лице по защита на данните прави периодичен преглед на първоначално вписаните данни в регистъра, преглежда вписаната информация и при необходимост коригира и допълва същата.

Раздел девети ОЦЕНКА НА ВЪЗДЕЙСТВИЕ И ОПРЕДЕЛЯНЕ НА СЪОТВЕТНО НИВО НА ЗАЩИТА

Чл. 34. (1) Оценката на въздействието върху защитата на данните (ОВЗД) е процес, който цели да опише обработването на данните, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове.

(2) Водещ критерии при извършване на преценката е степента (нивото) на въздействие, при което нарушаването на поверителността, целостта или наличността на личните данни би оказало върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 35. Администраторът е наясно с рисковете, свързани с обработването на определени видове лични данни и извършва оценка на въздействието всеки път, когато съществува вероятност обработването „да породи висок риск за правата и свободите на физическите лица". За целта е разработена специална процедура.

Чл. 36. Администраторът определя „ниско ниво" на защита за Регистър „Персонал".

Раздел десети

ТЕХНИЧЕСКИ И ОРЕАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ.

СЪХРАНЕНИЕ И ДОСТЪП ДО ДАННИТЕ

"т. а Ъ

Чл. 37. (1) Администраторът предприема пакет от технически и организационни мерки за защита на личните данни, за да гарантира адекватно ниво на защита, което отговаря на обработваните данни и въздействието при нарушаване на защитата им.

(2) Мерките по ал. 1 имат за цел да гарантират поверителност, цялостност и наличност на личните данни и обхващат физическа, персонална, документална защита, защита на автоматизирани информационни системи и/или мрежи и крпптографска защита.

Чл. 38. (1) Физическата защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сградата и помещенията, в които се обработват данните.

(2) Основните организационни мерки на физическа защита включват:

1. определяне на помещения, предназначени за самостоятелна работа на обработващия/оператора на лични данни, в които са разположени елементите на комуникационно-информационните системи, необходими за обработването;

2. определяне на организация на физическия достъп;

3. определяне на режим на посещения - допускат се единствено за целите на осъществяване на контрол на работния процес от страна на администратора и при осъществяване на нормативно установени задължения, които се прилагат спрямо получател на данните, в предвидените в закон случаи;

4. определяне на използваните технически средства за физическа защита;

5. определяне на екип за реагиране в случай на нарушение на сигурността на данните - при неправомерно проникване в помещенията, в които се обработват лични данни.

(3) Основните технически мерки на физическа защита се изразяват в:

1. осигуряване на специални шкафове, в които се съхраняват документите, съдържащи лични данни и които се поставят в определените за целите на обработка на данните помещения. Личните данни се обработват в работните помещения, в които се намират основните работни места на оправомощените лица и които са с ограничен достъп - само за тях.. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове в същите работни помещения. Помещенията, в които се обработват лични данни от регистъра са защитени чрез заключване на вратите. Достъп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистъра. Никое длъжностно или трето лице няма право на достъп до личните данни, освен ако те не са изисквани по надлежен законен път от органи на съдебната власт (съд, прокуратура, следствени органи). В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, администраторът на лични данни е длъжен да информира лицето, но не и да препятства работата на органите на съдебна власт, j j ,]

2. оборудване на съответните зони, с необходимите устройства за ограничаване на физическия достъп, с пожароизвестителни и пожарогасителни системи;

3. работата с компютърни системи е подсигурена с анти вирусни програми, пароли за достъп;

Чл. 39. (1) Персоналната защита представлява система от организационни мерки спрямо обработващите лични данни лица, като при постъпване на работа всички служители и наети лица биват запознати с тях, за удостоверяване на което подписват нарочен документ, и се изразява в:

1. познаване на нормативната уредба в областта на защитата на личните данни;

2. познаване на политиката и ръководствата за защита на личните данни;

3. знания за опасностите за личните данни, обработвани от администратора;

4. забрана за споделяне на лични данни и критична информация между субектите на данни (например идентификатори, пароли за достъп и т.н.);

5. съгласие за поемане на задължение за неразпространение на личните данни - обработващите лични данни подписват декларация за не разгласяване на лични данни, до конто са получили достъп при и/или по повод изпълнение на задълженията си;

6. преминато обучение за защита сигурността на данните.

(2) Мерките за персонална защита гарантират достъпа до лични данни само на обработващи лични данни лица или на такива, чиито законови задължения налагат такъв достъп, при спазване на принципа *„необходимост да знае"*.

Чл. 40. (1) Документалната защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

(2) Основните мерки на документална защита са:

1. определяне на регистрите, конто ще се поддържат на хартиен носител;

2. определяне на целта за обработване на лични данни - на основание чл. 6, ал. 1 от Регламента.

3. регламентиране на достъпа до регистрите - съхраняват се в помещения с контролиран достъп, предназначени за самостоятелна работа на обработващия/оператора на лични данни;

4. определяне на срокове за съхранение - регламентирани в член 14 от Инструкцията;

5. разписване на процедури за унищожаване - съгласно чл. 14 от настоящата Инструкция;

6. процедури за проверка и контрол на обработването - администраторът редовно преценява и извършва оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

(3) Обработването се извършва само по време на редовното работно време. Достъпът е ограничен само за оправомощените лица в съответствие с принципа „Необходимост да се знае".

(4) Личните данни могат да бъдат размножавани и разпространявани от оправомощените служители само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

(5) След изтичане на срока за съхранение, всички документи се унищожават или анонимизират, за което се съставя протокол от назначена със заповед комисия.

Чл. 41. (1) Защита на автоматизираните информационни системи ит мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни и обхваща:

1. разписана политика за защита на личните данни, ръководства по защита и стандартни операционни процедури;

2. идентификация и автентификация, дейностите по обработване и съхранение на лични данни на електронен носител (твърд диск в мрежа) са подсигурени с антивирусни програми и пароли за достъп;

3. защита от вируси;

4. поддържане и развитие на софтуерен продукт;

5. управление на конфигурацията;

6. създаване на копия/резервни копия за възстановяване на данните;

7. ясно описание на носителите на информация;

(2) Компютрите са със защитен достъп до личните данни. Системата за достъп поставя ограничения при опити за получаване на неоторизиран достъп до файловете с лични данни. Прави се електронен архив. Всеки оправомощен 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.

(3) Администраторът гарантира, че при пренос данните не могат да се четат или променят при пренасянето им.

(4) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено от оторизирани лица с определено ниво на достъп.

(5) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без предоставяне на достъп до личните данни.

(6) Не се разрешава осъществяването на отдалечен достъп до данни.

Чл. 42. (1) Достъпът до данните и разкриването на личните данни се осъществяват при условията и по реда на Общия регламент за защита на данните от:

1. субектите на данните, в съответствие с разпоредбата на член 15 от ОРЗД;
2. обработващия личните данни по смисъла на член 28 от ОРЗД;
3. получателя на данни;
4. надзорния орган в предвидените случаи.

(2) Администраторът предоставя на посочените в ал. 1 от този член лица лични данни в изпълнение на нормативно установени задължения.

(3) Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.): При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(4) Оправомощените служители следва да извършват ежегодни проверки на личните данни с оглед нивото на защита, преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението - за заличаването им.

Раздел единадесети
СИГУРНОСТ НА ОБРАБОТВАНЕТО. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 43. Администраторът гарантира сигурността на данните чрез въведени процедури за осигуряване на съобразено с нивото на риск на обработването ниво на сигурност с оглед естеството, обхватът, контекстът и целите на обработването, в строго съответствие с приложимото българското и европейско законодателство за конфиденциалност и защита на личните данни.

Чл. 44. (1) В случай на нарушение на сигурността на личните данни (настъпване на инцидент, в резултат на който се нарушава поверителността, наличието или целостта им, и има вероятност това нарушение да представлява риск за правата и свободите на дадено лице), администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган (КЗЛД), освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

(2) Уведомлението до надзорния орган съдържа причините за забавянето, в случаите когато не е подадено в срок от 72 часа от узнаването.

(3) Обработващият лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

Чл. 45. Уведомлението до надзорния орган има следното минимално съдържание:

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

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

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

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Чл. 46. В случай, че и доколкото не е възможно цялата необходима информация да бъде подадена едновременно, същата може да се подаде поетапно без по-нататъшно ненужно забавяне.

Чл. 47. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с последното.

Раздел дванадесети СЪОБЩАВАНЕ НА СУБЕКТА НА ДАННИТЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 48. (1) В случаите, когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, посочено в алинея 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията за контакт с администратора, описание на евентуалните последици от нарушението на сигурността на личните данни и описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително и мерките за намаляване на евентуалните неблагоприятни последици.

Чл. 49. Съобщението до субекта на данните не се изпраща в следните случаи:

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

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

в) то би довело до непропорционални усилия. В такъв случай администраторът прави публично съобщение или взема друга адекватна мярка, осигуряваща еднаква по степен и ефективност информираност на субектите на данни.

Раздел тринадесети ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

, Чл. 50. (1) При осъществяване на дейността на администратора не се извършва трансфер на лични данни за трети страни извън ЕС.

(2) При възникнала необходимост от предоставяне на лични данни извън рамките на ЕС, Администраторът ще предприеме всички необходими действия, посочени в чл. 44 и следващите от Общия регламент за защита на данните, с оглед осигуряването на подходящо ниво на защита на данните.

Чл. 51. За целите на настоящата Инструкция:

„Администратор на лични данни" е Институт по молекулярна биология при БАН адрес: 1113 София, ул. «Акад. Г. Бончев» бл. 21, стая 403 телефон: 02 872 35 07 ел. поща:. imb@bio21.bas.bg

Данни за контакт с длъжностното лице по защита на данните:

Мери Лалева Джонджурова

служебен адрес:

Институт по молекулярна биология-БАН, 1113 София, ул. «Акад. Г. Бончев» бл. 21, стая 401

телефон:02 872 80 50 ел. поща: pdadmin@bio21.bas.bg

(2) Данни за контакт с Работодателя в качеството му на администратор на данни: Доц. Ива Угринова - Директор на Институт по молекулярна биология-БАН адрес: 1113 София, ул. «Акад. Г. Бончев» бл. 21, стая 403 телефон: 02 872 35 07 ел. поща:. imb@bio21.bas.bg

Настоящата Инструкция е приета на 01.06.2018 г. и е сведена до знанието на всички служители на ИМБ - БАН.