



АГРАРЕН УНИВЕРСИТЕТ

Пловдив 4000; Бул. Менделеев № 12; Тел. +359/32/654300; Факс +359/32/633157

www.au-plovdiv.bg

AGRICULTURAL UNIVERSITY

Bulgaria, 4000 Plovdiv, 12 Mendeleev Str., Tel. +359/32/654300; Fax +359/32/633157

ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ АГРАРЕН УНИВЕРСИТЕТ – ПЛОВДИВ

ПРЕДМЕТ

Чл. 1. (1) Настоящите **Правила за защита на личните данни в Аграрен университет – Пловдив („Правилата“)**, определят реда, по който Аграрен университет - Пловдив (АУ – Пловдив), БУЛСТАТ00455464, наричан по-долу за краткост **„Университета“** събира, записва, организира, структурира, съхранява, използва, разкрива, подрежда, комбинира, ограничава, изтрива, унищожава и обработва лични данни за целите на своята дейност.

(2) В зависимост от конкретната ситуация **Университета** обработва данни в качеството на администратор на лични данни или обработващ лични данни.

(3) Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица и са приети съгласно чл.25 „и“ и следващите от Закона за защита на личните данни.

Чл. 2. Настоящите **Правила** уреждат:

1. принципите, процедурите и механизмите за обработка на личните данни;
2. процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;
3. процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;
4. лицата, които обработват лични данни и техните задължения;
5. правилата за предаване на лични данни на трети лица в България и чужбина;
6. необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
7. техническите ресурси, прилагани при обработката на лични данни.

ДЕФИНИЦИИ

Чл. 3. За целите на настоящите **Правила** използваните понятия имат следното значение:

- **ЗЗЛД** – Закон за защита на личните данни.
- **КЗЛД** – Комисия за защита на личните данни.
- **ОРЗД** – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични

данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Длъжностно лице отговорно за защита на личните данни – лице, което е служител в **Университета** или изпълнява функции по поръчка, на което са възложени задълженията във връзка със защитата и процесите по обработка на лични данни, уредени в тези **Правила**.

Администратор на лични данни – физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни. В настоящите **Правила** „администратор“ обозначава **АУ-Пловдив**.

Обработващ лични данни – лице или организация, което въз основа на договор обработва лични данни, предоставени от **АУ-Пловдив**, за уговорените цели. В настоящите **Правила** **АУ-Пловдив** е и в качеството си на „обработващ“ лични данни спрямо лица, на които предоставя услуги съгласно договор.

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

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

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

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

Чл. 4. (1) **АУ-Пловдив** е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни при обработването на лични данни **АУ – Пловдив** спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл.5. (1) **Субект на личните данни** е физическо лице, което е:

1.в трудови и/или граждански правоотношения с **АУ – Пловдив**, в т.ч. и кандидати за работа;

2.обучаеми / студенти, докторанти, специализанти, вкл. и кандидат-студенти/;

3.контрагенти и партньори;

4.посетители и други физически лица, свързани с осъществяването на дейността.

(2) **АУ-Пловдив** събира, обработва и съхранява лични данни, необходими за осъществяване на дейността си като държавно висше училище по смисъла на Закона за

висшето образование, работодател, контрагент или партньор при съблюдаване изискванията на приложимото законодателство.

(3) **АУ-Пловдив** обработва следните категории данни:

1. **Данни на преподаватели, служители/работници, кандидати за работа:**

а) **физическа идентичност**: име; ЕГН/ЛНЧ, данни по лична карта и/или паспорт (номер, дата и място на раждане, постоянен и/или настоящ адрес, срок на валидност), телефон за връзка, електронна поща, банкова сметка. С документа за самоличност се проверява самоличността и валидността на съответните документи.

б) **образование** – документи за придобито образование, квалификация, правоспособност, академично развитие, когато се изискват за длъжността и др.

в) **медицински данни** – карта за предварителен медицински преглед при постъпване на работа, документи за здравословно състояние, документи за трудоустрояване, вкл.решения на ТЕЛК, медицински свидетелства, болнични листове и всяка прилежаща към тях документация;

г) **трудова дейност** – документи за месторабота, трудов стаж, възнаграждения, професионална биография.

д) **свидетелство за съдимост**, когато се изисква за заемане на длъжност съгласно нормативен акт

е) **други данни**, чието обработване е необходимо за изпълнение на правомощията като работодател

2. **Данни на студенти, докторанти, специализанти, вкл. и кандидат-студенти**

а) **физическа идентичност**: име; ЕГН/ЛНЧ/ЛИН, данни по лична карта и/или паспорт (номер, дата и място на раждане, постоянен и/или настоящ адрес, срок на валидност), месторождение и гражданство за чуждестранни лица, телефон за връзка, електронна поща, банкова сметка, данни за здравно осигуряване, застраховки образователно-квалификационна степен, европейско приложение, свидетелство за правоспособност, фотоизображения, оценки от изпити. С документа за самоличност се проверява самоличността и валидността на съответните документи.

б) **медицински данни** – документи за здравословно състояние (медицински свидетелства, болнични листове и всяка прилежаща към тях документация; медицинско свидетелство за чуждестранни студенти);

3. **Данни на контрагенти и партньори:**

а) **физическа идентичност**: име; ЕГН/ЛНЧ, данни по лична карта и/или паспорт (номер, дата и място на раждане, постоянен и/или настоящ адрес, срок на валидност), телефон за връзка, електронна поща, банкова сметка. С документа за самоличност се проверява самоличността и валидността на съответните документи.

б) **образование** – документи за придобито образование, квалификация и правоспособност, когато се изискват за доказване на изискуемия капацитет за изпълнение на договорните задължения, както и при участие в процедури за обществени поръчки, търгове и други специфични взаимоотношения съгласно действащото законодателство.

4. **Данни за посетители и други физически лица, свързани с осъществяването на дейността на Университета**

а) **физическа идентичност**: име; ЕГН/ЛНЧ, данни по лична карта и/или паспорт (номер, дата и място на раждане, постоянен и/или настоящ адрес, срок на валидност), телефон за връзка, електронна поща, банкова сметка фото и видео изображения . С документа за самоличност се проверява самоличността и валидността на съответните документи.

(4) АУ-Пловдив обработва чувствителни данни, само доколкото това е необходимо за изпълнение на специфичните ѝ права и задължения в областта на трудовото и осигурително законодателство.

ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 6. АУ– Пловдив обработва лични данни за следните цели:

1. **осъществяване на обучението и администриране на учебния процес в Университета, вкл. кандидатстване и прием на студенти, докторанти и специализанти** – за индивидуализиране на документи за придобита образователна степен и квалификация; за всички дейности, свързани с изготвянето на надлежни документи съгласно държавните изисквания във връзка с обучението; за поддържане на съответните регистри съгласно Закона за висшето образование, Закона за развитие на академичния състав и правилниците към тях; за социално-битово обслужване, финансови отношения, достъп до ресурси за обучение на студенти, докторанти и специализанти и ефективна комуникация с тях във всичките ѝ форми във връзка с учебния процес;

2. **управление на човешките ресурси** – за индивидуализиране на трудовите и граждански правоотношения и всички дейности, свързани с тяхното възникване, именение и прекратяване, както и изготвяне на съответните за това документи / договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др./; за изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя за удържане и плащане на здравни и социални осигуровки и данъци; за установяване на връзка и кореспонденция във всичките ѝ форми с лицата във връзка с изпълнение на задълженията им по трудовите и граждански правоотношения, както и на други правомощия на Университета в качеството ѝ на работодател; за предоставяне на информация на Националния център за информация и документация съгласно Закона за развитие на академичния състав в Република България и правилниците към него, за избраните на академични длъжности лица и придобилите научна степен „доктор на науките”;

3. **сключване и изпълнение на договори с контрагенти и партньори на АУ-Пловдив** - за индивидуализиране на физически лица и персонализиране на юридически лица в граждански и търговски правоотношения и партньорски взаимоотношения с АУ – Пловдив.

Чл. 7. Принципите за защита на личните данни са:

1. **Законосъобразност, добросъвестност и прозрачност** - обработване при наличие на законово основание, при полагане на дължимата грижа и при предварително информиране на субекта на данни;

2. **Ограничение на целите** – събиране на данни за конкретни, точно определени и законни цели и не се обработват допълнително по начин, несъвместим с тези цели;

3. **Свеждане на данните до минимум** – данните да съответстват на целите, за които се събират и да са ограничени до необходимото във връзка с целите на обработването;

4. **Точност** – личните данни трябва да са точни и при необходимост да се актуализират при отчитане на целите на обработването, респ. да се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват

5.Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6.Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7.Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 8. За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

1. субектът на данните е дал своето съгласие;
2. обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
3. обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
4. обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;
5. обработването е необходимо за изпълнение на задача от обществен интерес;
- 6.обработването е необходимо за целите на легитимните интереси на администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни. Целите, за които се обработват лични данни на това основание, са описани в приложимите известия по защита на данните.

СЪГЛАСИЕ

Чл. 9. (1) Субектът на данни е съгласен с обработването, ако изрази това ясно и недвусмислено – чрез изявление или друг потвърждаващ акт. Ако съгласието за обработка на лични данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси. При заснемане и излъчване на публични събития и церемонии на **Университета**, се счита, че субектите на данни са дали своето съгласие с присъствието си, ако администраторът публично, ясно и недвусмислено е обявил това обстоятелство преди началото на събитието или церемонията.

(2) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

(3) С оглед спазването на принципа на отчетност декларациите за съгласие се съхраняват от **АУ-Пловдив**, докато се извършват действия по обработване на данни на това основание.

ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедура за обработване на личните данни на лицата, заети по трудови правоотношения в АУ-Пловдив

Чл. 10. (1) Личните данни на лицата, заети по трудови правоотношения в **АУ-Пловдив**, вкл. кандидатите за работа, се събират при и по повод набирането на персонал на основание и съгласно изискванията на Кодекса на труда и подзаконовите му нормативни актове, Закона за развитие на академичния състав в Република България и правилника за прилагането му, Правилника за устройството и дейността на АУ - Пловдив и Правилник за прилагане на ЗРАС в АУ-Пловдив. Данните на всеки работник и служител се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в зависимост от нуждата.

(2) Личните досиета се подреждат в специални картотечни шкафове, находящи се в кабинета на лицето, отговорно за личните данни на персонала. Данните на кандидатите за работа, които се съхраняват на хартиен носител, се съхраняват в нарочни шкафове. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, като за целта се създава специален ред за влизане в помещението чрез ключ, охрана чрез СОТ и парола.

(3) Личните данни за академично израстване се съхраняват в специални картотечни шкафове, находящи се в кабинета на експерт към УИЦ. Достъпът до кабинета се предоставя само на лицата, оправомощени да обработват личните данни, като за целта се създава специален ред за влизане в помещението чрез ключ.

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

(5) Досиетата на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградите на **Университета**.

Процедура за обработване на лични данни на контрагенти и партньори

Чл. 11. (1) Личните данни на контрагенти и партньори се събират при подаване на заявка за предоставяне на услуга или сключване на договор.

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

(3) Личните данни се съхраняват на електронен и/или хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Досиетата се съхраняват в шкафове в помещение с контролиран достъп в отдели ФСО и МО. Електронните данни се съхраняват в бази данни.

Процедура за обработване на лични данни на студенти, докторанти, специализанти, вкл. кандидат-студенти

Чл.12 (1) Личните данни на студенти, докторанти, специализанти, вкл. и кандидат-студенти, се събират при и по повод кандидатстването за обучение в **Университета** на основание и съгласно изискванията на Наредбата за държавните изисквания за приемане на студенти във висшите училища в Република България,

Наредбата за държавните изисквания към съдържанието на основните документи, издавани от висшите училища, Закона за развитие на академичния състав в Република България и правилника за прилагането му, Закона за висшето образование, ПМС № 90/26.05.2000г. за условията и реда за предоставяне на стипендии на студентите, докторантите и специализантите от държавните висши училища и научни организации, Наредба за ползване на студентските общежития и столове.

(2) Личните данни се съхраняват:

- данни свързани с учебния процес - в помещенията на учебен отдел, ДЕСП, кабинет на експерт - докторанти и кабинет на експерт международно сътрудничество;
- данните за социално-битово обслужване - в кабинета на личен състав;

Процедура за обработване на лични данни на посетители и други физически лица, свързани с осъществяването на дейността на Университета

Чл.13.(1) Личните данни на посетители и други физически лица, свързани с осъществяването на дейността на **Университета**, се събират при или по повод посещения, участие в публични събития и церемонии и др. изяви, когато е възможно и фото и/или видео заснемане на събитията и тяхното излъчване в и/или публикуване на интернет страницата на **Университета** и медии.

(2) Личните данни се съхраняват в помещение с контролиран достъп и СОТ.

ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 14. (1) **Университетът** документира дейностите по обработване на лични данни като спазва принципа на отчетност.

(2) Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

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

1. целите на обработването;
2. категориите лични данни и категориите субекти на данни;
3. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;
4. предаването на лични данни на трета държава;
5. когато е възможно, предвидените срокове за изтриване на различните категории данни;
6. общо описание на техническите и организационни мерки за сигурност.

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

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

Чл.15.(1) **АУ-Пловдив** води вътрешни регистри относно дейностите по обработване на лични данни по чл.30 от ОРЗД.

(2) Регистърът на лични данни е структурирана съвкупност от лични данни, достъпна по определени критерии съобразно настоящите правила, която е централизирана или децентрализирана и разпределена на функционален принцип.

(3) АУ – Пловдив поддържа следните регистри:

а) **РЕГИСТЪР „СТУДЕНТИ”** – създава се и се поддържа от „Учебно информационен център” по силата на възлагане с длъжностната характеристика за трудовата функция.

б) **РЕГИСТЪР „ДОКТОРАНТИ”** – създава се и се поддържа от експерт - докторанти по силата на възлагане с длъжностната характеристика за трудовата функция.

в) **РЕГИСТЪР „ПЕРСОНАЛ”** – създава се и се поддържа от експерт личен състав по силата на възлагане с длъжностната характеристика за трудовата функция.

г) **РЕГИСТЪР „КОНТРАГЕНТИ И ПАРТНЬОРИ”** - създава се и се поддържа от финансов контролор по силата на възлагане с длъжностната характеристика за трудовата функция.

Чл.16. (1) Право на достъп до регистрите с лични данни имат само органите на АУ - Пловдив съобразно възложените им от закона правомощия и оторизираните работници и служители, както и обработващи лични данни, на които администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

(2) Оторизирането на работници и служители се извършва с длъжностната характеристика за съответната трудова функция.

(3) Работниците и служители носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни.

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

(5) Всяко виновно нарушение от страна на оторизираните работници и служители на правилата и ограниченията за достъп до личните данни, както и разпространяването на информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения, се счита за неизпълнение на трудовите задължения и е основание за налагане на дисциплинарно наказание по реда на Кодекса на труда.

МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Технически мерки

Чл. 17. (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа. Възможните технически средства за контрол на достъпа са охрана на помещенията, охрана на сградата, политика на допускане на външни лица до помещенията само с придружител от персонала на висшето училище.

(2) Помещенията на **АУ-Пловдив** са надеждно обезопасени посредством противопожарни мерки съгласно българското законодателство.

Мерки за документална защита

Чл. 18. (1) **АУ-Пловдив** установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани в тези **Правила**. За отделни категории данни може да се предвиди псевдонимизиране по предложение на лицето, отговорно за личните данни.

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

Персонални мерки на защита

Чл. 19. (1) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:

1. поемат задължение за неразпространение на личните данни, до които имат достъп;
2. се запознават с нормативната база, вътрешните правила и политики на **Университета** относно защитата на личните данни;
3. преминават обучение за реакция при събития, застрашаващи сигурността на данните;
4. са инструктирани за опасностите за личните данни, които се обработват от **Университета**;
5. се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с тези **Правила** ред.

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните и обучение относно задълженията на дружеството, свързани с обработката на лични данни, както и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодически, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

Мерки за защита на автоматизирани информационни системи и криптографска защита

Чл. 20. (1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

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

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

Чл. 21. (1) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия, др., се осигурява посредством:

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

(2) Лицето, отговорно за личните данни, докладва периодически на ръководството на **Университета** предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 22. (1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на лицето, отговорно за личните данни, като му предоставят цялата налична информация.

(2) Лицето, отговорно за личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Лицето, отговорно за личните данни, докладва незабавно на ръководството на **Университета** наличната информация за нарушението на сигурността, включително информацията относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(4) След съгласуване с ръководството на **Университета**, лицето, отговорно за личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, лицето, отговорно за личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай лицето, отговорно за личните данни, уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

Чл. 23. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на **Университета** лицето, отговорно за личните данни, организира уведомяването на КЗЛД.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД съдържа следната информация:

а) описание на нарушението на сигурността; категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) името и координатите за връзка на лицето, отговорно за личните данни;

в) описание на евентуалните последици от нарушението на сигурността;

г) описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, лицето, отговорно за личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл. 24. (1) **Университета** води регистър на нарушенията на сигурността, който съдържа следната информация:

а) дата на установяване на нарушението;

б) описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);

в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за **Университета**;

д) предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(2) Регистърът се води в електронен формат от лицето, отговорно за личните данни.

ПРЕДОСТАВЯНЕ И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 25. (1) **Университета** има право при необходимост да предоставя или разкрива лични данни на:

1. физическите лица, за които се отнасят данните;

2. на компетентни органи на държавна и местна власт, институции и ведомства, които по силата на нормативен акт имат право да изискват предоставяне на информация, в т.ч. и лични данни – Съд, Прокуратура, Министерство на образованието и науката, МВР, НАП, НОИ и др.

3. лица, обработващи личните данни от името и по възлагане от АУ – Пловдив въз основа на изричен писмен договор /предоставящи услуги по организиране, съхраняване, поддържане и унищожаване на архиви с данни на обучаеми и работещи в **Университета**, банки, обслужващи плащанията и студентското кредитиране, служба по трудова медицина и др./. Същите са длъжни да обработват предоставените им лични данни при спазване на настоящите **Правила** и само за целите на възложената им работа.

4. висши училища/научни организации/други организации – партньори по съвместни образователни програми и проекти /национални и международни/ при спазване на приложимото законодателство и настоящите **Правила**.

(2) В случаите на предоставяне и обработване на данните на обучаващи се, служители, контрагенти и партньори, **Университета**:

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

б) гарантира в качеството си на обработващ спазване на законовите изисквания и утвърдените практики за обработка и защита на личните данни

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

г) сключва писмено споразумение или друг правен акт с администратора, който урежда задълженията на дружеството да обработва лични данни съгласно Регламент (ЕС) 2016/679;

д) информира физическите лица, чиито данни ще бъдат предоставени на обработващ.

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

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

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

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

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

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 26. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от **Университета**. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:

а) първоначалното въвеждане на нови технологии или прехода към нови технологии;

б) автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;

в) обработване на чувствителни лични данни в голям мащаб;

г) мащабно, систематично наблюдение на публично обществена зона.

(3) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 27. (1) Унищожаване на личните данни се извършва от **Университета** или изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

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

(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина или предаване съгласно Закона за националния архивен фонд и подзаконовите актове свързани с архивите. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

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

Чл. 28. Лицето, отговорно за личните данни, и лицата, обработващи личните данни от името на **Университета**, са физически или юридически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите **Правила**.

Чл. 29. Лицето, отговорно за личните данни /ДЛПЛД/:

1. подпомага **Университета** и лицата, обработващите личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;

2. осигурява нормалното функциониране на гореспоменатите системи за защита;

3. осъществява контрол през целия процес на събиране и обработване на данните;

4. изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

5. периодически изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;

6. уведомява ръководството на **Университета** своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;

7. унищожава данните от хартиените и техническите носители съгласно закона и сроковете, установени в тези **Правила**;

Чл. 30. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

(2) При възлагане на дейности, налагащи обработката на лични данни от регистрите на **Университета**, контрагентите следва да спазват приложимите нормативни изисквания относно обработката на личните данни и процедурите по тези **Правила**.

(3) При изпълнение на дейности, свързани с обработване на данни при предоставяне на услуги от страна на **Университета**, следва да бъдат спазвани приложимите нормативни изисквания относно обработката на лични данни.

(4) Достъп до личните данни могат да имат и съответните държавни органи в рамките на техните правомощия по закон – съд, следствие, прокуратура, ревизиращи и др. Гореспоменатите могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл.31. (1) Всяко лице има право да иска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

(2) Правото на достъп се осъществява чрез искане на засегнатото физическо лице, получено на адреса по седалището на **Университета** или официалната електронна поща.

(3) Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.

(4) Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

(5) **Университетът** е длъжен в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако се установи, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.

(6) Субектите на данни имат също правото да:

а) оттеглят съгласието си за обработване по всяко време;

б) възразят срещу употреба на личните им данни за целите на директния маркетинг;

в) изискат информация за основанието, въз основа на което личните им данни са предоставени за обработване на обработващ извън ЕС/ЕИП;

г) възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;

- д) бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
- е) подават жалби до регулаторния орган;
- ж) в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

СРОКОВЕ ЗА СЪХРАНЯВАНЕ НА ЛИЧНИ ДАННИ

Чл.32. (1) Като администратор на данни **Университетът** съхранява данни за период с минимална продължителност съгласно целите за обработка и предвиденото в действащото законодателство в съответствие с принципа за *ограничение на съхранението*.

(2) Данните, свързани с трудово правни и осигурителни отношения, в т.ч. ведомости и ведомости за възнаграждения на специализанти; договорите с хонорувани преподаватели, гост-преподаватели и чуждестранни преподаватели; гражданските договори се съхраняват за срок от 50 години.

(3) Протоколите от държавни изпити и защита на дипломни работи на студенти, протоколи от изпити на специализанти и главни книги се съхраняват постоянно в Университета.

(4) Досиетата на български студенти, съдържащи лична информация се съхраняват 1 година след придобиване на образователно-квалификационна степен, а на чуждестранните студенти – 3 години след придобиване на образователно-квалификационна степен

(5) Ведомостите за платени стипендии се съхраняват 10 години.

(6) Общите и индивидуални протоколи от изпити се съхраняват 5 години след придобиване на образователно-квалификационна степен.

(7) Документи за конкурси, процедури по подбор и назначаване и др. подобни се съхраняват до 6 м. освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок. След изтичането на този срок работодателят или органът по назначаването изтрива или унищожава съхраняваните документи с лични данни, освен ако специален закон предвижда друго.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 33. Всички работещи по трудови правоотношения в АУ - Пловдив са длъжни да се запознаят с настоящите **Правила** и да ги спазват при изпълнение на трудовата си функция и на възложената им работа. При виновно неизпълнение на задължения по настоящите **Правила** носят дисциплинарна отговорност по реда на Кодекса на труда.

Чл. 34. (1) За всички неуредени в настоящите **Правила** въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

(2) Приложение към настоящите **Правила** са образци на следните документи, съставяни при и по повод обработката на лични данни:

- **Приложение № 1** – Декларация-съгласие за обработка на лични данни, която се подписва, когато обработването не се извършва на друго основание, предвидено в чл. 6 от Регламент 2016/679;

- **Приложение № 2** – образец Протокол за задължителен инструктаж за запознаване с правилата за Противопожарна безопасност;

- **Приложение № 3** – образец на Протокол за унищожаване на лични данни и носители на лични данни;
- **Приложение № 4** – Споразумение за обработка на данни;
- **Приложение № 5** – Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите в АМТИИ – Пловдив правила и мерки за защита на личните данни;
- **Приложение № 6** – Искане за достъп до лични данни

Настоящите Правила са утвърдени със Заповед №РД-16423/21.03.2024г. на Ректора на АУ-Пловдив.