ВЪТРЕШНИ ПРАВИЛА ЗА СИГУРНОСТ ПРИ РАБОТА С РЕГИСТРИ С ЛИЧНИ ДАННИ В УНИВЕРСИТЕТ "ПРОФ. Д-Р АСЕН ЗЛАТАРОВ" - БУРГАС

Утвърдил:
/Ректор Проф. д-р М. Миткова/

Съдържание

I. ОБЩИ ПОЛОЖЕНИЯ 4

II. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ 4

III. ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ВОДЯТ В УНИВЕРСИТЕТ "Проф. д-р АСЕН ЗЛАТАРОВ" 5

IV. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ 8

V. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ 9

VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ 10

VII. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ 12

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ 12

Информация относно Администратора на лични данни, длъжностните лица по защита на личните данни и надзорния орган по защита на личните данни

Информация относно Администратора на лични данни

Наименование	Университет „Проф. д-р Асен Златаров" - Бургас
БУЛСТАТ	000044541
Седалище и адрес на управление	бул. „Проф. Якимов" № 1, гр. Бургас, България
Адрес за кореспонденция	бул. „Проф. Якимов" № 1, гр. Бургас, България
Телефон	(056) 86 00 41
Уебсайт	https://www.btu.bg/

Информация относно компетентния надзорен орган защита на личните данни

Наименование	Комисия за защита на личните данни
Седалище и адрес на управление	гр. София 1592, бул. „Проф. Цветан Лазаров" № 2
Адрес за кореспонденция	гр. София 1592, бул. „Проф. Цветан Лазаров" № 2
Телефон	02 915 3 518
Интернет страница	www.cpdp.bg

По смисъла на тези Вътрешни правила:

„Администратор на лични данни" е Университет "Проф. д-р Асен Златаров", представляван от Ректора на Университета.

„Обработващлични данни" са длъжностни лица от Университета, определени със Заповед на Ректора.

1.

I. ОБЩИ ПОЛОЖЕНИЯ

чл. 1. Настоящите вътрешни правила уреждат условията и реда за водене на регистри по Закона за защита на личните данни (ЗЗЛД), както и организацията и реда за упражняване на контрол при обработването на лични данни от преподавателите и служителите на Университет „Проф. д-р Асен Златаров" - Бургас.

Обработване на личните данни е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

Обработване на личните данни се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

чл. 2. Вътрешните правила се приемат с цел да регламентират:

- Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
- Видовете регистри, които се водят в Университета и тяхното описание.
- Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).
- Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.
- Процедури за докладване, управляване и реагиране при инциденти.

чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и се издават на основание на Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.

чл. 4. Университет „Проф. д-р Асен Златаров" - Бургас Бургас е **администратор на лични данни** по смисъла на чл.3, ал.1 от Закона за защита на личните данни.

чл. 5. Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

II. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

чл. 6. Администраторът възлага обработването на личните данни на негови служители. Обработването се възлага на повече от един служител, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на

конкретните им задължения.

Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

чл. 7. Личните данни в регистрите се набират от обработващият лични данни, които са предоставени от лицето-притежател на личните данни устно с интервю, на хартиен носител или чрез файл, предоставени от друг администратор на лични данни в съответен формат.

За необходимостта от набирането на данните и целите, за които ще бъдат използвани, обработващият данните информира лицето, след което се предоставят на ресорния ръководител на хартиен носител. Ако намери за необходимо ресорният ръководител, съгласува решението си с длъжностните лица, упражняващи оперативен и цялостен контрол.

За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки в определени шкафове и не се изнасят от сградата на администрацията на Университета, освен от обработващия лични данни, при служебна необходимост и на технически носител. Обработващият лични данни архивира въведените личните данни ежедневно или процедурата по архивиране е автоматизирана и се извършва в Компютърния център на Университета.

III. ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ВОДЯТ В УНИВЕРСИТЕТ "Проф. д-р АСЕН ЗЛАТАРОВ"

Регистри	**Лични данни, които се съдържат в регистъра**	**Отдел/Звено, в които се обработват личните данни**
1. Регистър на служителите по трудово правоотношение	- име, презиме, фамилия; - ЕГН; - пол; - дата на раждане; - постоянен адрес; - адрес за кореспонденция; - месторождение; - семейно положение; - гражданство; - инвалид да/не; - домашен телефон; - служебен телефон; - личен телефон; - банкови сметки; - снимка.	Човешки ресурси Компютърен център
2. Регистър на академичния състав	- ЕГН; - име, презиме, фамилия;	Човешки ресурси

1.

3. Регистър на заплатите и хонорари	- име, презиме, фамилия; - ЕГН; - номер на лична карта; - постоянен адрес ; - банкови сметки.	Финансово-счетоводен отдел Компютърен център
4. Регистър на заявленията за настаняване в общежитие	- ЕГН; - име, презиме, фамилия; - номер на лична карта; - дата на издаване; - от кого е издадена ЛК; - постоянен адрес; - факултетен номер - личен телефон; - имената на двамата родители; - адрес на родителите.	Инспектор социално-битови въпроси
5. Регистър на заявленията за кандидатстване за социални степендии	- ЕГН; - име, презиме, фамилия; - номер на лична карта; - дата на издаване; - от кого е издадена ЛК; - факултетен номер; - имената на двамата родители; - адрес на родителите; - документи за доказване на доход; - банкови сметки.	Инспектор социално-битови въпроси
6. Регистър н а регистрираните читатели в библиотеките на Университета	- ЕГН; - име, презиме, фамилия; - постоянен адрес; - личен телефон; - е-мейл.	Библиотека и филиали

1.

7. Регистър на обучаваните в Университета	- тип идентификация; - идентификация (ЕГН/ЛНЧ/СН); - име, презиме, фамилия; - дата на раждане; - пол; - месторождение; - гражданство; - местоживеене; - адрес по местоживеене; - данни от личната карта; - телефон; - е-мейл адрес; - социален статус: (болничен, майчинство, пълен сирак, ТЕЛК 70%); - второ гражданство.	Учебно-информационен център Компютърен център
8. Регистър на дипломираните	- регистрационен номер на дипломата; - дата на регистриране; - уникален индентификационен номер на дипломата; - име, презиме, фамилия; - факултетен номер; - ЕГН; - образователно - квалификационна степен; - специалност;	Учебно-информационен център
9. Регистър за здравното осигуряване на обучаваните	- ЕГН; - фамилия и инициали;	Компютърен център
10. Регистър на кандидат-студентите в Университета	- ЕГН - име, презиме, фамилия; - постоянен адрес; - телефон.	Учебно-информационен център Компютърен център
11. Регистър на заявленията за достъп до лична информация	- име, презиме, фамилия; - адрес за кореспонденция; - за студентите - факултететн номер - личен телефон; - е-мейл.	Канцелария

1.

12. Регистър за видеонаблюдение	**Филмови материали, относно достъпа на лица на територията на Университета**	Охрана

IV. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ

чл. 8. Форма на организация и съхраняване на личните данни на хартиен носител:

- Папките са разположени върху работните бюра и в офис шкафове в кабинетите на служителите, които се заключват. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри се контролира от ръководителите на отдели.
- Местонахождение на картотечния шкаф - може да бъде поставен в помещение, предназначено за самостоятелна работа на обработващия лични данни или в общо помещение за работа с изпълняващи други дейности.
- Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез:

- устно интервю с лицето;
- хартиен носител - писмени документи (заявления) по текущи въпроси в процеса на работа, подадени от лицето;
- външни източници (съдебни, финансови, осигурителни, данъчни и др. институции в изпълнение на нормативни изисквания).

- Личните данни от лицата се подават до администратора на личните данни Университет "Проф. д-р Асне Златаров", представляван от Ректора на Университета и длъжностното лице, определено за обработване на лични данни със Заповед на Ректора.
- Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана в т.VI на настоящите Вътрешни правила.

чл. 9. Форма на организация и съхраняване на личните данни на технически носител:

- Личните данни се въвеждат в база данни на сървър от компютърната мрежа или на отделен компютър. Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни
- При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.

- Достъп до файловете за обработка на лични данни имат само работещите с нея. Носители с лични данни могат да се разпространяват само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.
- Сървърите на които се съхраняват и обработват лични данни се намират в специално сървърно помощение в Компютърния център. Отделните компютри се намират в изолирано помещение за самостоятелна работа на обработващия лични данни по регистъра или в общо помещение с изпълняващи други дейности без право на достъп до него на останалите служители.
- Достъп до файловете за обработка на лични данни има само Лице, определено със Заповед на Ректора, обработващо лични данни чрез парола за отваряне на тези файлове, известна на него.
- Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва от отговорен служител от звеното по „Информационно обслужване и технологии". Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър, обработващ лични данни.

V. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

чл. 10. Програмно-апаратни мерки за гарантиране нивото на сигурност:

- компютърните сървъри за базите данни в Университета да са на съвременно техническо ниво. Сървърния хардуер да използва RAID технологии за дискова подсистема, hot-swap твърди дискове и оперативна памет с механизъм за откриване и корекции на грешки;

- компютърните работни конфигурации да използват операционни системи съобразно изискванията на приложния софтуер за работа с лични данни.

За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахранващи устройства (UPS).

Минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва:

- съвременна операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани последни пакети за сигурност;

- антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;

- активирана защитна стена и изграждане на ревърсни прокси сървъри за осигуряване на защитетн отдаличен достъп до системите на Университета.

Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица, които притежават съответните пароли, които се предоставят от Компютърния център съобразно политиката за избор на пароли в

Университета.

чл. 11. Физически мерки за гарантиране нивото на сигурност:

В помещенията, в които са разположени компютърни и комуникационни средства, следва да се осигури:

- система за ограничаване на достъпа;
- СОТ.

Всички работните помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран.

Всички магнито-оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорен и водоустойчив шкаф, който се заключва, а ключът се съхранява от ръководител звено Компютърен център. Контролът по използването на тези носители се извършва от ръководителя на посоченото звено.

чл. 12. Организационни мерки за гарантиране нивото на сигурност:

- Организира се охрана на работните помещения в рамките на охраната на цялата сграда (оперативни дежурни) и СОТ.
- Забранено е използването на преносими лични носители на данни в звената от университетската администрация, в които се обработват лични данни.
- Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- Проверка на всички работни компютърни конфигурации по чл. 5, ал. 1, т. 10 от Наредбата за минималното ниво на техническите и организационни мерки и допустимия вид защита на личните данни се извършва на всеки шест месеца от ръководителя на съответното звено и от отговорен служител от Компютърен център.
- Пренасянето на лични данни чрез интернет се осъществява чрез електронна поща, като задължително се осигурява криптиране на данните.
- При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.
- Със Заповед Ректорът определя обработващите лични данни за различните видове регистри.

VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

чл. 13. Служителите от Университет "Проф. д-р Асен Златаров" са длъжни да спазват и изпълняват Вътрешните правила, в съответствие с длъжностните им характеристики.

чл. 14. При обработване на личните данни служителят подписва декларация, че е запознат със ЗЗДЛ, относно механизма на обработване на лични данни и защитата им от незаконни форми на обработване, както и с настоящите Вътрешни правила.

чл. 15. Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

Лични данни се предоставят служебно между отделите на Университета след обосновано искане, чрез докладна записка от ръководителя на съответния отдел.

1.

чл. 16. Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в Университет "Проф. д-р Асен Златаров".

Правото на достъп се осъществява с писмено заявление/или заявление по електронен път по реда на Закона за електронните документи и електронния подпис/ до Ректора, лично или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно. Подаването на заявлението е безплатно.

Заявлението съдържа:

- име, адрес и други данни за идентифициране на съответното физическо лице;
- описание на искането;
- предпочитана форма за предоставяне на информацията;
- подпис, дата на подаване на заявлението и адрес за кореспонденция;
- приложено пълномощно, когато заявлението се подава от упълномощено лице.

Заявлението се завежда в канцеларията на Университета.

Достъп до данните на лицето се осигурява под формата на:

- устна справка;
- писмена справка;
- преглед на данните от самото лице или от упълномощеното такова;
- копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

При подаване на заявление за осигуряване на достъп до лични данни, представляващият администратора – Ректорът и упълномощените от него зам.-кмет и секретар по ресори разглеждат заявленията и разпореждат на обработващия лични данни да осигури искания достъп от лицето в предпочитаната от него форма.

Срокът за разглеждане на заявлението и произнасянето по него е 14- дневен от деня на подаването му. Срокът може да бъде мотивирано удължен до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

Администраторът уведомява писмено заявителя за решението си - то може да бъде за предоставяне на достъп или отказ за достъп. Уведомяването става лично срещу подпис или по пощата с обратна разписка.

Отказът на достъп до лични данни трябва да бъде мотивиран. Основанията за отказ са:

- когато данните не съществуват;
- когато данните не могат да бъдат предоставяни на определено правно основание.

За отказ се счита и липсата на уведомление.

Отказът за предоставяне на достъп до лични данни може да се обжалва от лицето в съда.

Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на Ректора обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.

Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите на лицата началници на отдели, декани, директори, замл ректори отговарящи за съответния ресор, в който се водят регистри. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

чл. 17. Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

I.

При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.

Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третото лице в 30 - дневен срок от подаване на искането.

VII. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

чл. 18. При възникване и установяване на инцидент веднага се докладва на лицето, отговорно за защита на личните данни;

За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

След анализ, в дневника се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

В случаите на компрометирането на парола тя се подменя с нова, като събитието се отразява в дневника за инциденти.

ДОПЪЛНИТЕЛНИРАЗПОРЕДБИ

Вътрешните правила се приемат на Академичен съвет и се утвърждават, допълват, изменят и отменят от Академичния съвет по предложение на Ректора на Университет „Проф. д-р Асен Златаров" - Бургас .

Вътрешните правила влизат в сила от деня на тяхното утвърждаване. РС 46/20.06.201

1.