БУРГАСКИ ДЪРЖАВЕН УНИВЕРСИТЕТ “ПРОФ. Д-Р АСЕН ЗЛАТАРОВ”

Бургас 8010, бул. “Проф. Якимов” № 1
тел. (056) 716 407; 359886688640; e-mail: rector@btu.bg

Утвърдил:
Ректор
/Проф. д-р Сотир Сотиров/

БДУ
"ПРОФ. Д-Р АСЕН ЗЛАТАРОВ"

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА СЛУЖИТЕЛИТЕ

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	БДУ „Проф. д-р Асен Златаров“ -
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) 9308 200
Уебсайт	https://www..bg/
Регистрация на администратор на лични данни в КЗЛД	157688

Информация относно длъжностното лице по защита на личните данни

Име	Николай Димитров Паунчев
Адрес за кореспонденция	бул. „Проф. Якимов“ № 1, гр. Бургас, България
Телефон	
E-mail	nikolai_paunchev@abv.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

1. Предназначение, обхват и ползватели

Тази политика урежда управлението на личните данни, свързани със служителите на **БДУ „Проф. д-р Асен Златаров“**, (наричан по-долу “Университет”) и предоставя правила и процедури, които се прилагат за всички отдели и лица в рамките на Университета, с цел да се гарантира, че са защитени правилно във всички държави и региони.

Тези правила се отнасят за обработката на лични данни на служителите от всеки отделен отдел или физическо лице, в рамките на Университета, във всички страни и региони.

Потребителите на този документ са всички служители на Университета.

2. Референтни документи

- EU GDPR 2016/679 (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО)
- Закон за защита на личните данни
- НАРЕДБА № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни
- Политика за защита на личните данни
- Политика за съхранение на данни
- Политика за нарушаване на данни
- Политика за трансгранично прехвърляне на данни
- Процедура за нарушаване на данни

3. Дефиниции

Следните определения на термините, използвани в този документ, са дефинирани в Общия регламент относно защита на данните на Европейския съюз:

„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

Чувствителни лични данни: Личните данни, които по своята същност са особено чувствителни по отношение на основните права и свободи, заслужават специфична защита, тъй като контекстът на тяхната обработка може да създаде значителни рискове за основните права и свободи. Тези лични данни включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикати, генетични данни, биометрични данни, с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни, отнасящи се до пола на физическо лице, живот или сексуална ориентация

Обработване: „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

Администратор на 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; 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.

4. Основни принципи за обработка на лични данни на служителите

4.1. Законосъобразност, честност и прозрачност

Личните данни на Служителите трябва да бъдат обработвани законосъобразно, справедливо и по прозрачен начин по отношение на служителите.

4.2. Ограничение на предназначението

Личните данни на служителите трябва да се събират за конкретни, изрични и законосъобразни цели и да не се обработват по начин, който е несъвместим с тези цели.

4.3. Минимизиране на данните

Личните данни на служителите трябва да бъдат адекватни, уместни и ограничени до това, което е необходимо във връзка с целите, за които се обработват. Университета трябва да прилага анонимност или псевдонимация на личните данни на служителите, когато това е възможно, за да се намалят рисковете за съответните служители.

4.4. Точност

Личните данни на служителите трябва да бъдат точни и, при необходимост, актуализирани; трябва да се предприемат разумни стъпки, за да се гарантира, че неточните лични данни, като се имат предвид целите, за които се обработват, се изтриват или коригират своевременно

4.5. Ограничение на сроковете за съхранение

Личните данни на служителите трябва да се съхраняват не повече от времето, необходимо за целите, за които се обработват личните данни, в съответствие с Политиката за съхранение на данни.

4.6. Почтеност и поверителност

Вземайки предвид състоянието на технологиите и другите налични мерки за сигурност, разходите по внедряването, вероятността, и тежестта на рисковете за неприкосновеността на личния живот, трябва да се използват подходящи технически и организационни мерки за осигуряване на подходяща сигурност за личните данни, включително защита срещу случайно или незаконно унищожаване , загуба, промяна, неоторизиран достъп или разкриване.

4.7. Отговорност

Университетът, като администратор на данни за лични данни на служителите, отговаря и трябва да може да е в състояние да докаже съответствие с принципите, описани по-горе.

5. Законови цели за обработване на лични данни на служителите

Университетът може да обработва лични данни на служителите си за законни цели, които включват, но не се ограничават до:

Човешки ресурси и управление на персонала. Обхваща дейности по управление на човешките ресурси, извършвани като част от сключването или изпълнението на трудов договор (например: наемане на работа, прекратяване на договора, изпълнение на работен график и записи за присъствие, изпълнение на поставени задачи, компенсации, обезщетения и обучение).

Съответствие с местното законодателство и законите на държавите-членки на ЕС. Обхваща обработването на лични данни, когато това е необходимо, за да се изпълни правно задължение, на което Университета е подчинен. Целта му е да осигури спазването на закона от страна на Университета, включително, но не само - предотвратяването на престъпления и разкриването на лични данни на държавни институции и надзорни органи, включително данъчни и трудови органи.

Изпълнение на организационни процеси и вътрешно управление. Обхваща пътуване и разходи, свързани с управление на активи на Университета, ИТ услуги, информационна сигурност, провеждане на вътрешни одити и разследвания, правни или бизнес консултации и подготовка или разрешаване на спорове.

6. Изисквания за обработка на лични данни на персонала

Всяка обработка на лични данни на служителите на Университета трябва да бъде със законова цел и трябва да отговаря на следните изисквания:

6.1. Уведомяване на служителите

За целите на прозрачността на обработката на лични данни на служителите, те трябва да бъдат уведомени за типовете данни, които се събират, целта и видовете обработка, правата на служителя и мерките за сигурност, предприети за защита на личните данни. Уведомлението може да бъде под формата на публикуване или актуализиране на изявления за защита на личните данни на служителите, например: въвеждане на условия за защита на личните данни на служителите в трудови договори; Създаването на декларация за лични данни в съответните информационни системи.

6.2. Избор и съгласие на служителите

По принцип Университета може да обработва личните данни на служителите със законова цел като работодател и обикновено може да направи това без да получи съгласието на служителя, за да подобри ефективността на вътрешната работа.

Дейностите по управление на човешките ресурси, като например интервюта, назначаване, прекратяване на трудовото правоотношение, присъствие, компенсация и обезщетения, услуги за служителите, здраве и безопасност на труда могат да включват обработката на чувствителни лични данни. Ако законът или подзаконовите нормативни актове уреждат тези въпроси (например получаване на съгласието на служителя), Университетът ще вземе под внимание тези

закони или подзаконови актове. Юридическите отдели отговарят за определянето на специфични изисквания за спазване; отделите за човешките ресурси са отговорни за осигуряването на съответствие.

6.3. Събиране

Личните данни на служителите се събират за законови цели и трябва да се спазват принципа за минимизиране на данните. Ако личните данни на кандидат за работа или служител са събрани от трета страна (напр. Агенции за набиране на персонал), Университета трябва да полага всички усилия, за да си гарантира, че третата страна е получила личните данни с легитимни средства. Университетът не може да събира лични данни на кандидатите за работа или служителя по начин, който е в противоречие със закона.

6.4. Използване, съхранение и премахване

Физическите лица, работещи за Университета, трябва да използват, задържат и да се разпореждат с личните си данни по начин, който съответства на уведомлението на служителя. Те също така трябва да гарантират тяхната точност, цялост и уместност. Те трябва да предприемат подходящи мерки за сигурност, за да защитят личните си данни от случайно или незаконно *унищожаване, загуба, промяна, неоторизиран достъп или разкриване,*относноистенността на информацията и други документи, които описват сигурността на данните.

Физическите лица не трябва незаконно да унищожават или да променят личните си данни. Те не трябва да осъществяват достъп, или предоставяне на лични данни на служители на трета страна незаконно или без разрешение.

Служителят по защита на данните ще реши дали личните данни на служителя ще бъдат обработвани, за да се сведе до минимум риска за защита на данните: личните данни на служителите могат да бъдат анонимизирани с цел необратима де-идентификация; или данните могат да бъдат обобщени в статистически резултати или резултати от проучвания. (Принципите за обработка на лични данни не важат за анонимни данни и обобщени данни, тъй като не са лични данни.)

6.5. Разкриване на информация на трети страни

Когато лицата, работещи в Университета, трябва да разкриват лични данни на служители на доставчик, партньор или друга трета страна, те трябва да се стремят да гарантират, че доставчикът, партньорът или друга трета страна ще предостави мерки за сигурност, за да защити подходящите лични данни на служителите към свързаните рискове. Те трябва също така да изискват от третата страна да предостави същото ниво на защита на данните като Университета, чрез договор или друго споразумение.

Освен това, когато се разкриват лични данни на служителите в отговор на искане от правоохранителна или съдебна власт, те първо трябва да уведомят Университета по правните въпроси, за да положат координирани усилия за справяне с искането.

6.6. Трансграничен трансфер на лични данни на служителите

Организациите, които работят в световен мащаб, прехвърлят и обработват персоналните данни на служителите по целия свят. Различните държави налагат различни изисквания за трансграничното прехвърляне на лични данни (като например ограничения, условно ограничение или забрана за прехвърляне на определени видове лични данни извън страната). Преди да прехвърлят лични данни извън дадена страна, отделите на Университета и физическите лица, работещи в него, трябва да се консултират със съответния служител по защита на данните или с отдела по правни въпроси, за да установят дали трансграничното прехвърляне е необходимо и законно.

При прехвърляне на лични данни на служителите извън Европейското икономическо пространство, прехвърлящият и придобиващият трябва да са подписали споразумение за трансфер на данни, в съответствие с разпоредбите на ЕС и политиката за трансгранично прехвърляне на данни. Придобиващият трябва да осигури адекватна защита на прехвърлените данни, в съответствие с договора за трансфер на данни.

6.7. Достъп на служители

Университетът трябва да осигурява разумни средства на служителите, които да имат достъп до личните си данни, както и да позволява на служителите си да актуализират, коригират, изтриват или предават своите лични данни, ако това е уместно или изисквано от закона. Когато отговаря на искане на служител за достъп, Университетът не може да предоставя никакви лични данни, докато не се потвърди самоличността на служителя. Университетът трябва да се увери, че знае самоличността на лицето, подало молбата, преди да може да изпрати личните данни на лицето.

7. Отговорности

Отдел Човешки ресурси е отговорен за управлението и съхранението на Личните Данни на Служителите.

8. Действия, в случай на несъответствие

Всяко лице/служител на Университета, което знае за нарушение на лични данни, включително лични данни на служители, трябва да го докладва на съответните отговорни лица в Университета. Когато е необходимо да съобщите за нарушение на данните извън Университета, моля, следвайте Политиката за нарушаване на личните данни.

Въпреки това, ако се изисква от местното законодателство на страната, в която е настъпило нарушението на данните, лицето, посочено в Процедурата за нарушаване на данните, трябва да докладва инцидента на регулаторния орган и/или заинтересованите страни, в рамките на отчетния период, определен от закона.

9. Отговорности

Всяко лице, което нарушава тази политика, може да бъде обект на вътрешни дисциплинарни действия (включително и прекратяване на неговата заетост); може също да бъде изправено пред гражданска или наказателна отговорност, ако действията му нарушават закона.

10. Изключения и вариации

Представители/Служители на Университета също трябва да спазват тази политика при обработката на личните данни на друг персонал. "Друг персонал" включва: (1) лица, търсещи работа в Университета; (2) лица, които преди това са били наети от Университета; (3) други служители на Университета, които работят в Университета (като служители на съдействащи партньори, консултанти, стажанти).

11. Собственик и контакти

Отделът за управление на човешките ресурси е собственик на тази политика и трябва да я тълкува и управлява.

12. Управление на записи съхранени на база на този документ

Име на записа	Място на съхранение	Отговорник за съхранението	Контроли за защита на записите
Досие на служител	Кабинет с осигурен контрол на достъпа Защитен сървър	Отдел Човешки ресурси Компютърен център	Само упълномощени лица имат достъп до досиетата

13. Валидност

14. Този документ се приема на Академичен съвет и се утвърждава, допълва, изменя и отменя от Академичния съвет по предложение на Ректора на БДУ „Проф. д-р Асен Златаров“ -

15. Той влиза в сила от деня на неговото утвърждаване.

Политиката е актуализирана с решение на АС № 61 на 28.05.2026г.

Технически секретар:
(доц. д-р Петя Стефанова)

Секретар:
(доц. д-р Полина Милушева)