# РУСЕНСКИ УНИВЕРСИТЕТ „АНГЕЛ КЪНЧЕВ“

Уважаеми Дами/ Господа,

Благодарим за проявения интерес към Политиката за защита на личните данни на Русенския университет „Ангел Кънчев“! Тя е разработена в съответствие с изискванията на Общия Регламент за защита на данните 2016/679- GDPR, който се прилага от 25 май 2018 година.

Държим да Ви информираме, че за да осъществява пълноценно своите функции нашето висше училище непосредствено и чрез някои от своите интранет уеб-базирани платформи събира определена информация от физическите лица, потребители на образователни и квалификационни услуги (кандидат-студенти, студенти, кандидат-докторанти, докторанти, курсисти, специализанти и др.); от участниците в научни прояви; от персонала (кандидати за постъпване на работа, хабилитирани и нехабилитирани, щатни и хонорувани преподаватели, работници и служители и др.) и страните по сключени договори (контрагенти).

Затова Ви молим, запознайте се с настоящата Политика за поверителност и в случай, че имате въпроси, свържете с Администратора, чрез определеното от него Длъжностно лице за защита на данните (ДЛЗД). Ако не сте съгласни с някои от условията, съдържащи се в нея, препоръчваме Ви, да не предоставяте личните си данни и да не ползвате уеб-базираните платформи на Университета.

Настоящата Политика за поверителност се прилага за Русенския университет „Ангел Кънчев“, всички негови структурни звена и филиали и по отношение на всички осъществявани дейности и предоставяни услуги.

# ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

## (Утвърдена със Заповед № 894/25.05.2018г. на Ректора на Русенския университет)

### I. ВЪВЕДЕНИЕ

Политиката за защита на личните данни на Русенския университет „Ангел Кънчев“, наричана също така „Политика за поверителност“ е разработена в съответствие с изискванията на Общия Регламент за защита на данните 2016/679- GDPR, който се прилага от 25 май 2018 година.

За да осъществява пълноценно своите функции, Русенският университет „Ангел Кънчев“, наричан „Университета“ или „Администратора“ непосредствено и чрез някои от своите интранет уеб-базирани платформи събира определена информация от физическите лица, потребители на образователни и квалификационни услуги (кандидат-студенти, студенти, кандидат-докторанти, докторанти, курсисти, специализанти и др.); от участниците в научни прояви; от персонала (кандидати за постъпване на работа, хабилитирани и нехабилитирани, щатни и хонорувани преподаватели, работници и служители и др.) и страните по сключени договори (контрагенти), наричани заедно или поотделно „Субекти“ или „Субекти на данните“.

Субектите следва внимателно да се да се запознаят с настоящата Политика за поверителност преди да встъпят в правоотношения с Администратора или да продължат да осъществяват функциите си по вече възникнали такива преди 25 май 2018 година. В случай, че имате въпроси, препоръчваме Ви да се свържете с Администратора, чрез определеното от него Длъжностно лице за защита на данните (ДЛЗД), а ако не сте съгласни с някои от условията, съдържащи се в Политиката за поверителност, препоръчваме Ви да не предоставяте личните си данни и да не ползвате уеб-базираните платформи на Университета.

Настоящата политика за поверителност се прилага за Русенския университет „Ангел Кънчев“, всички негови структурни звена и филиали и по отношение на всички осъществявани дейности и предоставяни услуги.

## II. ИНФОРМАЦИЯ ЗА АДМИНИСТРАТОРА

Администратор на лични данни е Русенски университет „Ангел Кънчев”, представляван от Ректора, със седалище и адрес на управление: град Русе, ПК 7017, улица „Студентска“ № 8, БУЛСТАТ 000522685, идентификационен № по ЗДДС: BG 000522685; уебсайт: http://www.uni-ruse.bg, e-mail: secretary@uni-ruse.bg, тел.: Ректорат: +35982888465, факс: +35982845708, вписан в регистъра на администраторите на лични данни, воден от Комисията за защита на личните данни под идентификационен № 0002987.

Русенският университет „Ангел Кънчев“ е създаден вследствие преобразуването на Висшето техническо училище „Ангел Кънчев“ в университет, съгласно решение на Народното събрание, обн., ДВ, бр.68 от 01.08.1995 година.

Към Администратора, обработващ лични данни са:

- Филиал на Русенския университет „Ангел Кънчев“ в град Видин с адрес: град Видин, улица „Бдин“ № 66;

- Филиал на Русенския университет „Ангел Кънчев“ в град Силистра с адрес: град Силистра, улица „Албена”№ 1;

- Филиал на Русенския университет „Ангел Кънчев“ в град Разград с адрес: град Разград, бул. „Априлско въстание” № 3;

и

Научноизследователски сектор при Русенския университет „Ангел Кънчев“ с адрес: град Русе, улица ”Студентска” № 8.

## III. ИНФОРМАЦИЯ ЗА НАДЗОРНИЯ ОРГАН

Надзорен орган по прилагането на Общия Регламент за защита на данните 2016/679- GDPR е Комисията за защита на личните данни (КЗЛД), адрес: София, ПК 1431, бул. „Акад. Иван Евстратиев Гешов” № 15, тел: +35929153518, Факс: +35929153525, уебсайт: http://www.cpdp.bg; e-mail: kzld@government.bg, kzld@cpdp.bg.

## IV. КООРДИНАТИ ЗА ВРЪЗКА С ДЛЪЖНОСТНОТО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Длъжностно лице по защита на данните на Русенски университет „Ангел Кънчев“ е А. Георгиев, адрес: град Русе, ПК 7017, улица „Студентска“ № 8, e-mail: dpo@uni-ruse.bg

## V. ЦЕЛИ И ОБХВАТ НА ПОЛИТИКАТА ЗА ПОВЕРИТЕЛНОСТ

Защитата на личните данни е важна за Университета. Затова Ви уверяваме, че се отнасяме сериозно и отговорно към защитата на Вашите лични данни и искаме да се чувствате сигурни и спокойни, както непосредствено при своето обучение, квалификация, специализация, научна работа, осъществяване на трудови функции или бизнес-контакти, а също така и при посещенията на нашия уебсайт и ползването на уеб-базираните платформи. Действията на Администратора са съобразени с приложимите законови разпоредби за защита на личните данни и сигурността срещу неоторизиран достъп до тях. Според възможностите си поддържаме най-високите технически и организационни мерки за сигурност, които предпазват предоставените ни от Вас лични данни от случайни или умишлени манипулации, загубване, увреждане или достъп на неоторизирани лица. Непрекъснато ще се стремим да подобряваме мерките за сигурност, следвайки добрите практики и технологичните новости.

Настоящата Политика за поверителност съдържа информация за целите на обработването на личните данни; видовете регистри с лични данни, водени от Администратора; механизмите на водене, поддържане и защита на регистрите, съхраняващи лични данни на лицата, заети по трудови или граждански правоотношения, или предоставени при други

договорни отношения с висшето училище, както и на кандидат-студенти, студенти и докторанти; задълженията на длъжностните лица- оператори на лични данни и техните отговорности при изпълнение на задълженията им; необходимите технически и организационни мерки за защита на личните данни; информация относно получателите или категориите получатели, на които могат да бъдат разкрити данните; информация относно данните за задължителния или доброволния характер на предоставяне на данните и последиците от отказ за предоставянето им; информация за правото на достъп и правото на коригиране на събраните данни и др.

## VI. ДЕФИНИЦИИ

Термините, които се използват в настоящата политика за поверителност имат следните значения:

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

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

- „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

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

- „псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

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

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

- „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

- „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.;

- „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;

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

- „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

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

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

- „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51 от Общия Регламент за защита на данните 2016/679- GDPR.

- „оператор на лични данни” е длъжностно лице, на което в съответствие със задълженията по длъжностна характеристика Администраторът е възложил непосредствено да изпълнява конкретните функции и дейности по събиране, обработка и съхранение на лични данни при условията и по реда, посочени в настоящата Политика за поверителност.

## VII. ПРИНЦИПИ СВЪРЗАНИ С ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

При обработването на лични данни Администраторът ще съблюдава принципите, заложени в чл.5 от Общия Регламент за защита на данните 2016/679- GDPR, регламентиращи общата рамка на защитата правата на физическите лица при обработване на техните лични данни, а именно:

- законосъобразност, добросъвестност и прозрачност; да има конкретност и изричност на целта и срока, за който ще се извършва (ограничение на целите);
- да бъде ограничено до целите на обработването (свеждане на данните до минимум);
- трябва да бъде точно и актуално (точност);
- съхранението на личните данни следва да бъде обвързано с определен срок само за целите на обработването (ограничение на съхранението);
- обработването трябва да гарантира подходящи нива на сигурност, чрез прилагане на технически или организационни мерки (цялостност и поверителност);
- Администраторът да може да докаже защо се събират и обработват данните (отчетност).

Обработването на личните данни е законосъобразно, когато е налице поне един от следните елементи при обработването:

- Субектът е дал съгласие за една или повече конкретни цели;

- е за изпълнение на договор, по който Субектът е страна;

- за спазване на законово задължение, приложимо спрямо Администратора;

- е за изпълнение на задача в обществен интерес;

- е за защита на жизненоважни интереси на Субекта на данните;

- е необходимо за легитимните интереси на Администратора, освен ако тези на Субекта не са с предимство, например когато субектът е дете.

Съгласието, дадено от Субекта трябва да е:

- недвусмислено;
- да може да бъде оттеглено по всяко време;
- да е свободно изразено, информирано и конкретно.

Съгласието може да бъде дадено в писмена декларация или в устна форма. Когато съгласието се дава от Субекта в писмена форма и е част от декларация, касаеща и други въпроси, то трябва да се отличава ясно от т.нар. друга част.

С настоящата политика за поверителност Администраторът информира Субектите, че съгласието за обработване на данните е оттегляемо по всяко време. Операторите на лични данни са обучени да уведомяват Субектите за това тяхно право от всеки път преди те да дадат съгласие за обработване на лични данни.

## VIII. ЦЕЛИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

В регистър „Персонал“ Администраторът събира и обработва лични данни на работещите по трудови правоотношения и на наетите по граждански договори, академичния състав, докторанти, включително архив на работилите в Университета със следните цели: индивидуализиране на страните по трудовите и гражданските правоотношения и на членовете на академичния състав и на обучаващите се докторанти; съхраняване на предоставените документи в предвидените срокове; изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за висшето образование- за периодично атестиране на членовете на академичния състав, Закона за развитие на академичния състав в Република България, Закона за задълженията и договорите, Закона за държавния архив, Закон за здравното осигуряване, Закона за счетоводството, Наредбата за допълнителните и други трудови задължения, Закона за държавния архив, Номенклатурата за водене и съхраняване на делата, Инструкцията да документооборота и др.; обработване на събраните данни за служебни цели, свързани със съществуване, изменение и прекратяване на трудовите и гражданските правоотношения, акредитиране на Университета, с изплащани на трудови възнаграждения по трудови и граждански договори, изплащане на обезщетения, внасяне на осигурителни вноски за държавното обществено и здравно осигуряване, изготвяне на справки, издаване на документи и други статистически и исторически цели и др.; организиране на обучението на докторантите; провеждане на конкурси за избор на хабилитирани и нехабилитирани членове на академичния състав, на докторанти и др.

Администраторът събира и обработва лични данни на кандидат-студенти и студенти в регистър „Учащи“. Регистърът съдържа данни за кандидатстващите за обучение в Университета и лицата придобили статус на студент, със следните цели: индивидуализиране на кандидат-студенти и студенти; изпълнение на нормативните изисквания на Закона за висшето образование, Наредбата за прием на български и чуждестранни граждани във висшите училища на Република България, Правилника за устройството и дейността на Русенски университет „Ангел Кънчев”, Правила за прием на студенти в Русенския университет, Закона за здравно осигуряване, Наредба за съдържанието на основните документи, издавани от висшите училища и др.; използване на събрани данни за служебни цели, свързани с провеждане на кандидатстудентски конкурсни изпити, оценяване на изпитните работи, класиране на кандидатите и записване на класираните кандидати; използване на събраните данни за организационни цели, свързани с провеждане на учебния процес, издаване на официални документи, удостоверяващи студентското им положение и обслужващи мобилността на студентите, както и издаването на дипломи;

Администраторът събира и обработва лични данни на физическите лица, сключили граждански договори и други видове договори с Университета и данни на настанени наематели в студентски общежития в регистър „Контрагенти” с цел индивидуализация на страните по правоотношението.

Администраторът събира и обработва лични данни на физически лица в „Библиотечен регистър“ с цел индивидуализация на Субектите, ползващи библиотечни услуги.

Администраторът събира и обработва лични данни на физически лица в регистър „Охрана и видеонаблюдение“ с цел осъществяване на пропускателния режим; идентификация на Субектите; охрана на собствеността и имуществото на Университета и опазване на обществения ред.

В посочените регистри Администраторът събира и обработва чувствителни данни[1] със следните цели:

- идентифициране на Субектите чрез лицевото изображение (фотоснимка) върху издадени от Администратора легитимационно-удостоверителни документи: служебна карта; студентска книжка, студентска лична карта; читателска карта; пропуск за студентско общежитие, като всички те се съхраняват от Субектите;

- идентифициране на Субектите чрез лицевото изображение (фотоснимка) върху заявление за кандидатстване в кандидат-студентски прием; личен студентски картон и/или главна книга; личен картон за настаняване в общежитие;

- идентифициране на Субектите чрез видеозаписите от камерите за денонощно видеонаблюдение;

- установяване на минималните национални изисквания към научната, преподавателската и/или художествено-творческата или спортната дейност на кандидатите за придобиване на научна степен и за заемане на академичните длъжности „главен асистент", „доцент" и „професор", определени в Закона за развитие на академичния състав, чрез събиране и обработване на наукометрични показатели, които отразяват научните резултати и техния отзвук в научната литература, и/или показатели, които отразяват измерими постижения в художествено-творческата или спортната дейност и показатели, които отразяват измерими академични резултати в преподавателската дейност, в т.ч. за преценка на научноизследователската работа на кандидатите за академичната длъжност „доцент“ и „професор“, чрез информация за членство в авторитетна творческа и/или професионална организация в съответната научна област; респ. за преценка на художественотворческата или спортната дейност чрез информация за членство в творческа организация;

- установяване на националността на Субектите, за да се установи законовото право на лицето да работи в Република България или за настаняването му в студентско общежитие;

- данни за здравословното състояние- необходимо е да се предоставят за заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, както и при необходимост на съобразяване на условията на труд; освобождаване от обучение по физическо възпитание и спорт; участие в спортни клубове и др. подобни със специфичното здравословно състояние на лицето и в случаите, в които това се изисква от действащото законодателство;

- за длъжностите, свързани с материална отговорност- информация дали лицето не е лишено от право да заема такива длъжности чрез свидетелство за съдимост, като тези данни могат да бъдат обработвани единствено под контрола на официален орган или когато обработването е разрешеното от правото на ЕС или на държавата членка.

## IX. ПРАВНОТО ОСНОВАНИЕ ЗА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Правните основания за събиране и обработване на личните данни в регистър „Персонал” се съдържат в Кодекса на труда, Закона за висшето образование, Закона за развитие на академичния състав; Кодекса за социално осигуряване, Закона за задълженията и договорите, Закона за държавния архив, Закона за здравното осигуряване, Закона за счетоводството, Наредбата за допълнителните и други трудови задължения, Закона за държавния архив, Номенклатурата за водене и съхраняване на делата, Инструкцията да документооборота и др.;

Правните основания за събиране и обработване на личните данни в регистър „Учащи” се съдържат в Закона за висшето образование; Закона за развитие на академичния състав в Република България; Закона за физическото възпитание и спорта; Наредбата за прием на български и чуждестранни граждани във висшите училища на Република България, Правилника за устройството и дейността на Русенски университет „Ангел Кънчев”, Правила за прием на студенти в Русенския университет, Закона за здравно осигуряване, Наредба за съдържанието на основните документи, издавани от висшите училища и др.;

Правните основания за събиране и обработване на личните данни в „Контрагенти” се съдържат в Закона за задълженията и договорите; Закона за гражданската регистрация, Наредбата за ползване на студентските общежития и столове, Правилник за условията и реда за настаняване в студентските общежития и др.

[1] Съгласно член 4, параграфи 13, 14 и 15, член 9 и съображения (51)- (56) от Общия Регламент за защита на данните 2016/679- GDPR, личните данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения; членство в професионална организация; генетични данни, биометрични данни, обработвани единствено с цел идентификацията като човешко същество; данни за здравословното състояние и данни за сексуалния живот или сексуалната ориентация на дадено лице, се считат за „чувствителни“ и подлежат на специфични условия на обработване от Администратора.

Правните основания за събиране и обработване на личните данни в „Библиотечен регистър“ се съдържат в Закона за задълженията и договорите, Закона за закрила и развитие на културата, Закона за задължителното депозиране на екземпляри от печатни и други произведения; Правилника за прилагане на Закона за задължителното депозиране на екземпляри от печатни и други произведения.

Правните основания за събиране и обработване на личните данни в регистър „Охрана и видеонаблюдение“ се съдържат в Закона за частната охранителна дейност.

## X. ДАННИ, КОИТО СЕ СЪБИРАТ И ОБРАБОТВАТ

Университетът ще използва Вашите лични данни единствено за осъществяване на целите, за които те са предоставени, със знанието и предварително съгласие на Субектите. Администраторът ще събира и обработва лични данни, разпределени по регистри и типове, както следва:

В регистър „Персонал” Администраторът събира и обработва следните групи лични данни:

- Относно физическата идентичност на лицата: имена, ЕГН, данни от личната карта- номер, дата на издаване, място на издаване и срок на валидност, лицевото изображение (фотоснимка); адрес по местоживеене, телефон за връзка;

- Относно семейната идентичност на лицата: семейно положение- наличие на брак, развод, брой на децата в семейството и тяхната възраст;

- Относно образованието: степен на образованието, придобита специалност, допълнителна квалификация, научна степен, научно звание;

- Относно трудовата и научна дейност- професионална автобиография; данни от трудова книжка и/или служебната книжка;

- Относно здравословното състояние;

- Относно гражданскоправния статус на лицата: свидетелство за съдимост, в случаите предвидени в закон и съобразно целите за събиране и обработване на чувствителни данни, посочени по-горе;

- Относно икономическата идентичност: автобиография, работна заплата, допълнителни възнаграждения; осигурителен доход- неговите източници и размер; трудови и нетрудови доходи; размер на доходите; данни за банковите сметки.

- Относно научната дейност- професионална автобиография, научни публикации, научни разработки, членство в професионални организации и др.

В регистър „Учащи” Администраторът събира и обработва следните групи лични данни:

При кандидат-студенти:

- Относно физическата идентичност на лицата: имена, ЕГН, данни от личната карта- номер, дата на издаване, място на издаване и срок на валидност, лицевото изображение (фотоснимка); адрес и телефон за връзка;

- Относно образованието: учебно заведение, степен на образование, придобита специалност;

При студенти:

- Относно физическата идентичност на лицата: имена, ЕГН, адрес по местоживеене, постоянен адрес, лицевото изображение (фотоснимка); данни от личната карта- номер, дата на издаване, място на издаване и срок на валидност, телефон за връзка и др.;

- Относно семейната идентичност на лицата: семейно положение;

- Относно образованието: степен на образование, придобита специалност и други данни от дипломата; писмените отговори, дадени по време на изпит, и евентуалните коментари на изпитващия по тези отговори;

- Относно трудовата дейност: съществуват или не трудовоправни отношения;

- Относно здравословното състояние на студентите;

- Относно икономическата идентичност: данни за банковите сметки; осигурителен доход, неговите източници и размер; трудови и нетрудови доходи.

В регистър „Контрагенти” Администраторът събира и обработва следните групи лични данни:

- Относно физическата идентичност на лицата: имена, ЕГН, адрес по местоживеене, телефони за връзка, данни от личната карта- номер, дата на издаване, място на издаване и срок на валидност; лицевото изображение (фотоснимка);

- Относно семейната идентичност на лицата: семейно положение;

- Относно образованието: висше училище, факултет (филиал), специалност, курс, факултетен номер;

- Относно икономическата идентичност: размер на доходите.

В регистър „Охрана и видеонаблюдение“ Администраторът събира и обработва следните групи лични данни:

- Относно физическата идентичност на лицата: имена, ЕГН, номер на лична карта;

- Данни от автоматичното денонощно видеонаблюдение (видеообраз) за движението на Субектите към подходите към сградите, площадките, коридорите и паркинга на Университета. Видеонаблюдението се извършва от оператори на лични данни- пазачи в случаите на самоохрана или служители на търговец, осъществяващ частна охранителна дейност, с която Администраторът има сключен договор за охрана, чрез изградена система за видеонаблюдение с изведен образ при дежурните охранители. Записващо устройство съхранява записите до 60 дни, след което те автоматично се изтриват.

Администраторът събира и обработва следните чувствителни данни:

- биометрични данни: лицеви изображения (фотоснимка); видеоизображения от системата за автоматичното денонощно видеонаблюдение.

- данни за членство в професионални организации;

- лични данни, които разкриват произход: националност- данните съдържат информация за националността на лицата и са необходими, за да се провери законовото право на лицето да работи или да бъде настанено в студентско общежитие;

- медицински данни: медицинско свидетелство за започване на работа; болнични листове; медицински бележки. Данните са от значение при заемане на длъжности и изпълнение на функции по трудови правоотношения, изискващи висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, както и при необходимост на съобразяване на условията на труд или обучение със специфичното здравословно състояние на лицето и в случаите, в които това се изисква от действащото законодателство;

- данни за гражданскоправния статус на лицата: свидетелство за съдимост- за длъжностите, свързани с материална отговорност; тези данни могат да бъдат обработвани единствено под контрола на официален орган или когато обработването е разрешеното от правото на ЕС или на държавата членка.

Тъй като нашият стремеж е непрекъснато да развиваме дейностите, които осъществяваме и услугите, които предоставяме, възможно е да отправим до Вас запитване, дали сте съгласни да използваме Вашите лични данни, за да Ви предоставяме нови или допълнителни услуги или информация, напр.: за образователни, научни или културни събития, в т.ч. новини и информация за предстоящи събития в Университета; спонсорски или стипендиантски програми; безвъзмездни или възмездни стажантски програми; студентски, докторантски, или преподавателски обмен; публични лекции; семинари; бригади и др. подобни. Тези нови или допълнителни дейности и услуги по правило няма да имат търговска, рекламна или маркетингова насоченост. Чрез посочените допълнителни дейности и услуги ние целим единствено да популяризираме дейността на Университета и да изпълним поетите към Вас ангажименти и да Ви предоставим отношение, информация и услуги на нивото, което заслужавате и очаквате. В посочените случаи ние предварително ще Ви помолим да се съгласите да получавате информация от подобно естество. Независимо, че ще го правим с Вашето съгласие, Вие имате право по всяко време да откажете Вашите лични данни да продължат да бъдат използвани за тези допълнителни цели. В този случай можете да се отпишете като изпратите електронно писмо до автора на съобщенията или на e-mail: dpo@uni-ruse.bg.

Университетът може да използва Ваша информация, за да създава статистически справки, които са напълно анонимни, както и за да извършва статистически анализ въз основа на тези данни.

## XI. УКАЗАНИЯ ЗА ИЗПОЛЗВАНЕ НА БИСКВИТКИ

Чрез уебсайта: http://www.uni-ruse.bg Администраторът не събира никаква лична информация (например: име, адрес, телефон или e-mail).

При посещаване на уебсайта се събира техническа информация от Вашия компютър. Необходимата информация съдържа например вид на браузера, операционна система, име на домейна на Вашия интернет-доставчик. Става въпрос изключително за информация, която не допуска свързване с конкретна личност. Тази информация се събира анонимно и се използва за целите на статистическата обработка.

Когато посещавате нашия уебсайт, е възможно да запаметим на Вашия компютър информация във формата на Cookies, която Ви разпознава автоматично при следващото Ви посещение. Т.нар. “кукита“ ни позволяват да персонализираме посещението Ви или да запаметим паролата Ви, за да не я въвеждате всеки път. Ако не искате да

разпознаваме компютъра Ви, настройте интернет-браузера си така, че да изтрива Cookies от твърдия диск, да ги блокира или да Ви предупреждава преди да съхрани някой от тях.

Нашият уебсайт използва Google Analytics, това е услуга на Гугъл за уеб- анализ, Google вкл. Google Analytics използва Cookies. Това са текстови файлове, които се съхраняват на Вашия компютър и позволяват анализиране на използването на нашия уебсайт от Вас. Те съдържат информация за операционната система, за браузера, Вашия IP- адрес, посетените от Вас преди това уеб-сайтове (Refferer-URL) и датата и часа на Вашето посещение на нашия уебсайт. Получената чрез тези текстови файлове информация за използването на нашия сайт се прехвърля на сървър на Google в съответния регион (Европа) и там се запаметява. Google ще използва тази информация, за да оцени използването на нашия сайт, да изготви доклад за действията в уеб-страницата за съответните доставчици и за предоставяне на други услуги, свързани с използването на този уебсайт и на интернет. Google в никакъв случай няма да свързва IP- адреса Ви с други данни в Google. Доколкото има законови разпоредби в тази връзка или ако трето лице обработва данните по поръчение на Google, Google ще предостави данните и на това трето лице.

На уебсайта може да се съдържат линкове към други сайтове (“Електронни страници на трети страни“), които могат да Ви позволят да посетите други електронни страници. Ако решите да посетите някоя от тези страници на трети страни, като кликнете върху връзка или се придвижите към страница на трета страна, Вие ще бъдете пренасочени към страницата на съответната трета страна. Фактът, че ние предоставяме връзка към дадена електронна страница чрез уебсайта, или публикувайки рекламен банер или друг вид реклама, или Ви предлагаме възможност да взаимодействате с, или да предоставяте лична информация на трета страна, не е гаранция, позволение или представяне на нашата принадлежност към въпросната трета страна и не следва да бъде разглеждано като съгласие с техните политики и практики за поверителност и информационна сигурност. Обръщаме Ви внимание, че нашите IT- специалисти нямат влияние върху съдържанието на тези сайтове. Те са проверени внимателно преди пренасочването на линковете, поради което е малко вероятно, но въпреки това не е изключено, операторите на съответните страници да извършат промени в съдържанието, които да са в разрез с действащото законодателство или с философията на Русенския университет „Ангел Кънчев“. В подобни случаи Университетът се дистанцира от подобно съдържание.

## XII. ЗА КАКЪВ СРОК СЕ СЪХРАНЯВАТ ЛИЧНИТЕ ДАННИ

Администраторът ще ограничи до минимум срока за съхранение на личните данни. Този период ще е съобразен с причините, поради които Университетът трябва да обработва данните, както и с всички нормативни изисквания за съхранение на данните за определен период от време, в т.ч. произтичащи от трудовото, осигурително и данъчно законодателство, специалните нормативните актове в областта на образованието и науката, както и останалите закони, които предвиждат задължения личните данни да се съхраняват за определен период от време. По изключение личните данни могат да се съхраняват за по-дълъг период от време за целите на архивирането от обществен интерес или научни или исторически изследвания. В тези случаи Администраторът ще предприеме подходящи технически и организационни мерки за тяхната защита като анонимност, криптиране и т.н.

Дейностите на Университета във връзка със съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се осъществяват при условията и реда на Закона за националния архивен фонд и вътрешните правила на Университета, регламентиращи оборота и срока за съхранение на електронни документи, както и на документи на хартиен носител и други вътрешни документи на Администратора.

През периода за съхранение Администраторът периодично ще актуализира данните, за да ги поддържа точни.

След изтичането на срока за съхранение Администраторът ще унищожи данните, след като е била изпълнена целта, за която са били събрани. Съгласно чл.56, ал.4 от ЗЧОД, записите от техническите средства за видеонаблюдение се съхраняват в регистър "Видеонаблюдение" два месеца след изготвянето им. Унищожаването им се удостоверява от ръководителя на охранителната дейност.

## XIII. ЗАДЪЛЖИТЕЛЕН И ДОБРОВОЛЕН ХАРАКТЕР НА ПРЕДОСТАВЯНЕ НА ЛИЧНИТЕ ДАННИ

Източниците, от които се събират данните в регистър „Персонал“ са: Субектите, за които те се отнасят и се предоставят доброволно при постъпване на работа или при настъпване на изменения на трудовото правоотношение. Субектите дават съгласие личните данни, които не са изискуеми по закон да се събират и обработват за една или повече конкретни цели. Нормативните актове в областта на трудовото и осигурителното право, висшето образование и науката и

др. предвиждат задължение за Администратора да събира и обработва данните в регистър „Персонал“, поради което за тяхното събиране и обработване не е необходимо съгласието на Субектите. Отказът за предоставянето им се явява като пречка за настъпване на желаните правни последици.

Източниците, от които се събират данните в регистър „Учащи“ са: Субектите, за които те се отнасят и се предоставят доброволно. Субектите дават съгласие личните данни, които не са изискуеми по закон да се събират и обработват за една или повече конкретни цели. Нормативните актове в областта на висшето образование и науката предвиждат задължение за Администратора да събира и обработва данните в регистър „Учащи“, поради което за тяхното събиране и обработване не е необходимо съгласието на Субектите. Отказът за предоставянето им се явява като пречка за настъпване на желаните правни последици.

Източниците, от които се събират данните в регистър „Контрагенти“ са: Субектите, за които те се отнасят и се предоставят доброволно. Субектите дават съгласие личните данни, които не са изискуеми по закон да се събират и обработват за една или повече конкретни цели. Отказът на Субекта за предоставянето на данните се явява като пречка за настаняване в студентско общежитие или настъпването на други желаните правни последици.

Източниците, от които се събират данните в „Библиотечния регистър“ са: Субектите, за които те се отнасят и се предоставят доброволно. Субектите дават съгласие личните данни, които не са изискуеми по закон да се събират и обработват за една или повече конкретни цели. Отказът на Субекта за предоставянето на данните ще се явява като пречка за ползване на библиотечните фондове и услуги.

Източниците, от които се събират данните в регистър „Охрана и видеонаблюдение“ са: Субектите, за които те се отнасят и се предоставят доброволно от лицата преди влизането им в охраняемия обект. На видни места, в т.ч. на входовете на сградите на Университета са поставени информационни табели за уведомяване на гражданите, че при влизане и излизане от сградата на Университета подлежат на проверка и за използването на технически средства за наблюдение и контрол, съгласно чл.56 от ЗЧОД. Отказът за предоставянето им се явява пречка за посещение на охранявания обект.

## XIV. ИНФОРМАЦИЯ ОТНОСНО ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

Регистър „Персонал“ се води от Администратора, както следва:

1. На хартиен носител:

- Данните се набират в писмена (документална) форма и се съхраняват в личните досиета на всеки работещ в Университета, всеки член на академичния състав и на всеки докторант, и в папки;

- Архивните дела се съхраняват в писмена (документална) форма;

- Личните досиета и папките се подреждат в специални картотечни шкафове, които са разположени в отдел „Човешки ресурси”, отдел „Кадрови и научен потенциал” и Финансов отдел;

- Длъжностните лица- оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните досиета, в това число ограничаване на достъпа до тях от външни лица;

- Личните досиета не се изнасят извън сградите на Администратора.

2. На технически носител:

- Личните данни се въвеждат в база данни на твърдия диск и в отделни информационни файлове тип „електронна таблица” на компютрите на операторите на лични данни, които са свързани с локална мрежа, със защитен достъп. Непосредствен достъп имат само операторите на лични данни;

- Компютрите са изолирани в помещение за самостоятелна работа;

- Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране, както и поддържането на информацията на хартиен носител.

Регистър „Учащи” се води от Администратора или чрез възлагане на обработващи данните от името на Администратора, както следва:

1. На хартиен носител:

- Данните се набират в писмена (документална) форма и се съхраняват в папки и в специални шкафове;

- Длъжностните лица от учебен отдел- оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни на кандидат-студентите, в това число ограничаване на достъпа до тях на външни лица;

- Папките с досиетата на студентите се подреждат в шкафове, които са разположени в изолирани, заключващи се помещения на операторите на лични данни;

- Информацията от хартиените носители за всеки студент, се записва по отделни партиди в Главна книга със задължителни реквизити по образец, която се съхранява в същите изолирани помещения;

- Длъжностните лица- оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни на студентите.

2. На технически носител:

- Личните данни се въвеждат в програмно-генерирани информационни файлове на компютрите на операторите на лични данни и в централизирана база данни на твърдия диск на изолиран компютър, които са свързани в локалната мрежа, със защитен достъп до личните данни. Непосредствен достъп до базата данни имат само операторите на лични данни с дефинирани права на достъп до определени нива.

- Компютрите на операторите на лични данни са изолирани в помещения за самостоятелна работа;

- Защитата на електронните данни от неправомерен достъп се осъществява посредством съвременен комплекс от хардуерни и софтуерни редундантни защитни механизми- антивирусен мониторинг, криптирани архиви, както и чрез поддържане на информацията и на хартиен носител.

Регистър „Контрагенти" се води от Администратора, както следва:

1. На хартиен носител при видове договори:

- Данните се набират в писмена (документална) форма и се съхраняват в папки;

- Папките се подреждат в шкафове, които са разположени в заключващи се изолирани помещения;

- Длъжностните лица- оператори на лични данни предприемат всички организационно-технически мерки за съхранението и опазването на личните данни.

2. На технически носител:

- Личните данни се въвеждат в отделни информационни текстови файлове на компютрите на операторите на лични данни, които са свързани в локалната мрежа, със защитен достъп до личните данни. Непосредствен достъп имат само операторите на лични данни;

- Компютрите на операторите на лични данни са разположени в изолирани помещения за самостоятелна работа;

- Защитата на електронните данни от неправомерен достъп се осъществява посредством съвременен комплекс от хардуерни и софтуерни редундантни защитни механизми- антивирусен мониторинг, криптирани архиви, както и чрез поддържане на информацията и на хартиен носител.

3. На хартиен носител при студентски общежития:

- Данните на наемателите се вписват в настанителни картони и адресни карти, съгласно изискванията на МВР;

- Настанителните картони се съхраняват в специални шкафове, които са разположени в изолирани помещения, а адресните карти се предават в МВР;

- Длъжностните лица- оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазване на личните данни, в това число ограничаване на достъпа на външни лица;

- Настанителните картони на наемателите не се изнасят извън сградата на администратора.

4. На технически носител:

- Личните данни се въвеждат в програмно-генерирани файлове на компютрите на операторите на лични данни, които са свързани в локалната мрежа, със защитен достъп до личните данни. Непосредствен достъп имат само операторите на лични данни;

- Компютрите са изолирани в помещения за самостоятелна работа;

- Защитата на електронните данни от неправомерен достъп се осъществява посредством съвременен комплекс от хардуерни и софтуерни редундантни защитни механизми- антивирусен мониторинг, криптирани архиви, както и чрез поддържане на информацията и на хартиен носител.

„Библиотечният регистър“ се води от Администратора, както следва:

1. На хартиен носител:

- Данните се набират в писмена (документална) форма и се съхраняват в специални картотечни шкафове;

- Информацията от хартиените носители за всеки студент, се записва по отделни читателски партиди със задължителни реквизити по образец, която се съхранява в същите изолирани помещения;

- Длъжностните лица от университетската библиотека- оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни на Субектите, в това число ограничаване на достъпа до тях на външни лица;

2. На технически носител:

- Личните данни се въвеждат в програмно-генерирани информационни файлове на компютрите на операторите на лични данни и в централизирана база данни на твърдия диск на изолиран компютър, които са свързани в локалната мрежа, със защитен достъп до личните данни. Непосредствен достъп до базата данни имат само операторите на лични данни с дефинирани права на достъп до определени нива.

- Компютрите на операторите на лични данни са изолирани за самостоятелна работа.

- Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране, както и чрез поддържане на информацията и на хартиен носител.

Регистър „Охрана и видеонаблюдение“ се води от Администратора и/или чрез възлагане на обработващи данните от името на Администратора, както следва:**.**

1. На хартиен носител:

- личните данни на Субектите се водят на хартиен носител в прошнурован и преномериран дневник, който се съхраняват в помещението на охраната, което се заключва.

2. На технически носител:

- системата за денонощно видеонаблюдение се осъществява чрез технически средства за наблюдение и контрол, съгласно чл.56 от ЗЧОД;

- Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране, както и чрез поддържане на информацията и на хартиен носител.

## XV. ИНФОРМАЦИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1. Физическа защита- представлява система от мерки по защита на сградите и помещенията, в които се създават, обработват и съхраняват лични данни и контрола върху достъпа до тях;

1.1. Организационни мерки:

- Определяне на зони с контролиран достъп;

Всички физически зони с хартиени и електронни записи, са ограничени само за служители, които трябва да имат достъп до тях с оглед изпълнението на служебните им задължения. Всички записи и документи на хартиен носител, съдържащи лични данни, са в заключени шкафове, които са заключени в кабинети с ограничен достъп, достъпен само от упълномощен персонал;

- Данните са защитени чрез използването на средства за физически контрол на достъпа, като заключване на вратите. Всички помещения, в които се съхраняват данни на хартиен носител, се намират в зони с ограничен достъп са защитени чрез заключване на вратите, заключване на контейнерите или други подобни средства. Електронни носители включително сървъри, са защитени по подобен начин, в зони с контрол на климата. Обектът и неговите помещения са защитени с 24-часова физическа охрана и охрана с технически средства;

- Определяне на помещенията, в които ще се обработват лични данни.

Личните данни се обработват в непублична част от помещенията, която е физически ограничена и достъпна само за служители, за които е необходимо да имат достъп с оглед на изпълнението на служебните им задължения. Личните данни на служителите се обработват от звеното „Човешки ресурси“, достъпът до които е ограничен само до оторизираните лица;

- Определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;

Комуникационно-информационните системи, използвани за обработка на лични данни са отделени от общодостъпните зони и са физически защитени, като достъпът е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните;

- Определяне на организацията на физическия достъп:

Физически достъп до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи, е възможен само през заключени врати. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения, след оторизация;

1.2. Определяне на техническите средства за физическа защита:

- Технически мерки, в т.ч. охрана със СОТ;

- Ключалки и оборудване на помещения;

Ключалки се използват, за да осигурят защита на зони, в които се съхраняват оборудване и лични данни. Тези зони, са достъпни само чрез ключ.

Помещенията, които съдържат лични данни са защитени чрез заключване на вратите и/или заключване на шкафовете. Заключените врати са достъпни чрез ключ, за защита от неоторизирани лица.

Помещенията, в които се съхраняват регистри с лични данни само на хартиен носител са оборудвани със СОТ, пожароизвестителна и пожарогасителна техника. Документите съдържащи лични данни, се съхраняват в заключени картотеки, като всички са в зоните с ограничен достъп на обекта, както е описано по- горе;

Шкафове с ограничен достъп се намират в звената, осъществяващи дейностите по управление на човешките ресурси, факултетните канцеларии, финансово- стопански дейности и др. Те по подразбиране са заключени, с цел защита на регистрите с лични данни;

- Пожарогасителни средства: в съответствие със закона, осигурени за защита на помещенията.

2. Персонална защита.

- Правната уредба на зашитата на лични данни се разглежда в обучителната програма по въпросите за защита на личните данни, която трябва да бъде премината от служителите на Университета. Служителите са длъжни да се запознаят с политиката за поверителност при първоначално възлагане на функциите на оператор на лични данни, както и да преминават през периодично обучение най-малко веднъж годишно. Университетът създава условия обучението да се извършва онлайн (електронно обучение), както и да е съобразено със спецификите на заеманите длъжности и звена;

- При възлагане на трудови функции като оператор на лични данни, служителите декларират, че се задължават да опазват и не разпространяват личните данни;

- Администраторът ще санкционира строго всяко виновно нарушаване на Политиката за поверителност от служителите.

- Служителите нямат право да споделят помежду си или с трети лица критично-важна информация, свързана със защита на личните данни (напр.: потребителски имена и пароли за достъп, както и ключове за достъп до помещения и шкафове за съхраняване на данни и др. подобни);

- Администраторът периодично извършва тренировки на персонала за реакция и процедура на действие при нарушение на сигурността на лични данни: тренировките представят в обучителна програма политиката за защита на личните данни; служителите се обучават да реагират, ако имат съмнение или им е станало известно нарушение на сигурността на личните данни като незабавно да уведомят прекия си ръководител и ДЛЗД.

- На служебните компютри не могат да бъдат инсталирани програми за комуникация, видеокомуникация и игри, както и да се съхраняват лични снимки, видеофайлове, сканирани копия на документи за самоличност и др. подобна информация за служителите;

- Служителите, на които е възложено да подписват служебна кореспонденция с електронен подпис, нямат право да го предоставят на свои колеги или трети лица.

3. Документална защита.

- Регистрите, които са определени да се съхраняват и обработват лични данни единствено на хартиен носител не се изнасят от помещенията, заснемат, копират или сканират;

- Личните данни се събират само с оглед на конкретно определената от него цел, за която Субектът е бил предварително информиран и е дал изрично съгласие като писмените съгласия се съхраняват от Администратора. Администраторът трябва да може да докаже с оглед на всеки конкретен случай и Субект защо се събират и обработват данните;

- Всеки тип данни се класифицира в съответствие с тяхното предназначение и характер и са защитени в съответствие с изискванията, посочени по-горе, а именно: записи на хартиен носител се съхраняват в заключен шкаф или контейнер и се намират в зоните и помещенията с ограничен достъп;

- Достъпът до личните данни е ограничен и се предоставя само на оправомощени лица- служители на Администратора или чрез възлагане на обработващи данните от името на Администратора;

- Общият контрол на относно законосъобразното осъществяване на дейностите по събиране и обработват данните се осъществява от Администратора.

- Ръководителите на основни звена в Университета са отговорни за законосъобразното събиране и обработване на данните и контрола на достъп до регистрите с лични данни, осъществяван от съответните звена. Те предлагат на Администратора да оторизира конкретни служители- оператори на лични данни, които за изпълняват трудовите си функции и задължения към Университета събират и обработват лични данни. В съответствие с принципа за отчетност те документират всяко действие по събиране и обработване на лични данни или предоставяне на достъп. Достъп до данните

се осъществява само при наличие на правно основание за предоставянето им и трябва да бъде ограничен само до конкретни, минимално необходими данни с оглед на целите;

- Съхраняването на данни трябва да е в съответствие с целите, за които са събрани данни и законоустановения срок. Личните данни се съхраняват от Администратора толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани или както се изисква от приложимото право. След изтичането на определения срок, данните трябва да бъдат унищожени по безопасен начин;

- Служителите на Администратора са обучени относно политиката срещу заснимане, копиране, сканиране и всяка друга форма на неправомерно разпространение на записи, съдържащи лични данни. Операторите на лични данни и всички служителите на Университета нямат право да заснемат, копират и сканират документи за самоличност (лични карти, паспорти и др.) на Субектите. Посочените действия ще се разглеждат от Администратора като виновно поведение и ще се санкционират, в зависимост от тежестта на нарушението, включително с прекратяване на трудовите правоотношения с провинилия се служител;

- След изтичане на сроковете за съхранение документи на хартиен носител, които съдържат лични данни, трябва да бъдат унищожени по сигурен начин, когато вече не са необходими за правно-значими цели чрез нарязване или чрез изгаряне. Ръководителите на основни звена, които съхраняват такива документи са отговорни за сигурното им унищожаване.

4. Защита на автоматизираните информационни системи и/или мрежи.

4.1. Идентификация и автентификация;

- С цел да се въведе достъп, се изисква мултипотребителските информационни системи да прилагат уникални потребителски акаунти и лични пароли за всеки потребител с акаунт за достъп до мрежата. Университетът има утвърдени правила за акаунтите и паролите, който съответства на политиката за защита на личните данни;

- Създаване на потребителски акаунт за всеки мрежов потребител се извършва по утвърдения за целта ред;

4.2. Служителите са лично отговорни за правилното използване на техните потребителски акаунти и пароли;

Ръководителите на основни звена са отговорни за разрешаването на потребителски акаунт на достъп до информационната система, съдържаща лични данни. Ръководителите на основни звена трябва да изготвят предложения за възлагане, отказ или отнемане на функциите на оператор на лични данни на определени служители;

4.3. Управление на регистрите;

- Общото управление и контрол на дейностите, свързани със законосъобразното функциониране на регистрите с лични данни се осъществява от Администратора.

- ДЛЗД осъществява консултативни функции в областта на защитата на личните данни; надзор по спазването на Общия Регламент за защита на данните 2016/679- GDPR в Университета; повишаването на осведомеността и обучението на персонала, както и други функции, възложени му от Администратора;

- Ръководителите на звена отговарят за законосъобразното функциониране на регистрите с лични данни, администрирани изцяло или отчасти от тези звена.

- Регистър „Персонал: Операторите на личните данни в този регистър се определят от Администратора. Служителите, чиято длъжност изисква да имат информация за данните, съдържащи се в него, разполагат с ограничен достъп до данните, съдържащи се в регистъра. ;

- Регистър "Учащи": Операторите на личните данни в този регистър се определят от Администратора. Служителите, чиято длъжност изисква да имат информация за данните, съдържащи се в него, разполагат с ограничен достъп до данните, съдържащи се в регистъра;

- Регистър "Контрагенти": Операторите на личните данни в този регистър се определят от Администратора. Служители, чиято длъжност изисква да имат информация за данните, съдържащи се в него, разполагат с ограничен достъп до данните, съдържащи се в регистъра;

- „Библиотечен регистър“: Операторите на личните данни в този регистър се определят от Администратора. Служители, чиято длъжност изисква да имат информация за данните, съдържащи се в него, разполагат с ограничен достъп до данните, съдържащи се в регистъра;

- Регистър "Охрана и видеонаблюдение": Управлението на регистъра се осъществява от Администратора в случай на самоохрана или от търговеца, на който е възложено да осъществява охраната на обектите на Администратора по реда на ЗЧОД. Служителите от ръководството на Университета, както и служителите, чиято длъжност изисква достъп до данните, съдържащи се в този регистър, разполагат с ограничен достъп до данните в този регистър;

4.4. Външни връзки/свързване:

- В Университета е изградена университетска компютърна мрежа (RUNet). Нейната дейност е регламентирана в Правилника за развитието и експлоатацията на университетската компютърна мрежа. Мрежата обединява компютърните ресурси на отделните катедри и звена на Университета; предоставя компютърни ресурси за общо ползване в Университета; дава възможност за ползване на Intranet (вътрешни) и Internet (външни) услуги; обслужва информационните системи използвани в Университета; подпомага и поддържа учебната и научно-изследователската дейност на Университета.

- Електронните комуникации като: компютърни мрежи; класове; връзка с Интернет и др., са съсредоточени в Центъра за информационно и компютърно обслужване (ЦИКО) и останалите обособени звена с назначени IT-специалисти. Те постоянно се обновяват и актуализират. Всички необходими софтуерни програми за учебния процес и научната дейност са лицензирани и до тях свободен достъп имат както преподаватели, така и служители, докторанти и студенти.

- Университетът членува в безжичната мрежа Eduroam, чрез която преподаватели и студенти могат да използват световната услуга Eduroam за WiFi достъп до мрежови ресурси за нуждите на изследователската и образователната дейност. С потребителско име и парола, академичната общност има възможност за мобилна Интернет връзка, независимо къде се намира потребителят, ако е в обсега на Eduroam WiFi покритие в над 2 500 научно-изследователски и образователни институции по света. Аналогично, гостите на Университета могат да получат достъп до ресурсите на мрежата без допълнителна регистрация, ако имат такава в своята институция.

- Освен мобилност, Eduroam осигурява на своите потребители и високо ниво на сигурност чрез използването на най-актуалните методи за криптиране и автентикация. Изградената с най-модерно оборудване мрежа е високоскоростна и резервирана. Тя има гигабитова скорост, благодарение на прокараните оптични трасета. Персоналът по поддръжка на мрежата има възможност за постоянен мониторинг на натовареността й.

- Всички вътрешни мрежи на Университета, включително локални мрежи и телекомуникационни връзки от точка до точка са определени като вътрешни мрежи на Администратора. Всички безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на Администратора, или всякакви мрежи, които не са под административния контрол на Администратора, се определят като Обществени мрежи;

- IT- специалистите на Университета осъществяват контрол на достъпа до вътрешната мрежа на Администратора и инсталират или одобряват инсталирането на всички устройства за достъп до мрежата и технологиите, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства или технологии, които могат да позволят достъп до вътрешните мрежи на Администратора. Администраторът има правото да одобрява или отхвърля всеки неоторизиран достъп до своите мрежови ресурси. На служителите е забранено инсталирането на неоторизирани устройства за достъп до вътрешните мрежи на Администратора без изричното одобрение на IT- специалистите;

- IT- специалистите на Университета поддържат актуална документация за мрежите на Администратора, включително, но не само, за мрежови диаграми, стандарти на конфигурация на устройства, описи на устройствата, ведомствени стандарти и други документи;

- Всички вътрешни мрежи на Администратора трябва да бъдат изолирани от всякакви обществени мрежи чрез използване на устройство "защитна стена". Всички входящи интернет връзки на вътрешните мрежи на Администратора трябва да бъдат изолирани чрез използването на операционната защитна стена. Защитната стена по подразбиране трябва да отказва целия трафик, освен изрично одобрения трафик;

- Хардуерът на Администратора, който съхранява информация, съдържаща лични данни и който е постоянно или периодично свързан с компютърни мрежи, трябва да има система за контрол на достъпа, базирана на парола. Независимо от мрежовите връзки, всяка самостоятелна хардуерна обработка на такава информация също трябва да използва одобрена система за контрол на достъпа, базирана на парола;

- Всички входящи връзки към хардуера на Администратора от външни мрежи трябва да бъдат защитени с одобрена система за контрол на достъпа, базирана на парола и трябва да бъдат защитени от мрежова защитна стена. Когато се използват компютри с хардуер на Администратора, служителите на Университета не трябва да установяват неразрешени връзки с обществени мрежи, включително интернет услуги;

- С изключение на извънредни ситуации, всички промени на вътрешните мрежи на Университета трябва да бъдат одобрени съгласно вътрешните процедури за въвеждане и контрол на промените;

4.5. Телекомуникации и отдалечен достъп;

- Отдалечен достъп: отдалечен достъп до вътрешни мрежи на Администратора може да бъде предоставен за оторизирани нужди. Процедурите за отдалечен достъп и инструментите за такъв достъп, трябва да отговарят на всички политики за сигурност. Всеки отдалечен достъп, осъществен чрез обществена мрежа като Интернет или безжична мрежа трябва да използва криптиращи технологии;

- На служителите може да бъде предоставен достъп до интернет, за да изпълняват служебните си задължения, но индивидуалният достъп може да бъде прекратен по всяко време по преценка на Администратора. Цялата информация, получена чрез интернет трябва да бъде под съмнение, докато не бъде потвърдена от надеждни източници. Служителите не трябва да предоставят информация относно Администратора, независимо дали съдържа или не лични данни, на каквато и да е публично достъпна компютърна система като Интернет, освен ако това е било одобрено от ръководителя на звеното, отговорен за личните данни и ДЛЗЛД;

4.6. Защита от вируси;

- Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира. Системният софтуер се контролира и се поддържа от оторизиран персонал, който осигурява непрекъснатата му работа и сигурност. Оторизираният персонал включва стандартни и базови конфигурации за защита на операционни системи, защитни стени, рутери и мрежови устройства, които трябва да се документират и съхраняват за всяка компютърна платформа, с която Администраторът оперира. Стандартните и базови конфигурации за защита трябва да бъдат одобрени от оторизиран специалист по информационни технологии;

- Хардуерът на Администратора трябва да работи и да бъде актуализиран с версии на одобрен антивирусен софтуер и вирусните дефиниции на компютрите да бъдат активирани. Потребителите не трябва да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции. Антивирусният мониторинг трябва да се използва, за да сканира целият софтуер и файлове с данни, идващи от или до трети страни или други групи на Университета. Членовете на екипа не трябва да избягват или да изключват сканиране на процесите, които биха могли да предотвратят предаването на компютърни вируси. Преносимите флопи и дискови устройства и други носители на данни, използвани от заразен компютър не трябва да се използват на друг компютър, докато вирусът не бъде успешно премахнат. Заразеният компютър също трябва да бъде незабавно изолиран от вътрешните мрежи. Антивирусните журнали трябва да се съхраняват в продължение на най-малко седем (7) дни;

4.7. Поддържане/ експлоатация;

- Администраторът периодично трябва да провежда оценки на сигурността, уязвимостта и тестове за проникване в системи и мрежи. Университетът трябва да провежда годишни оценки за сигурността на информацията и/или неприкосновеността на личните данни. Служителите не трябва да придобиват, притежават, търгуват или използват хардуерни или софтуерни инструменти, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Примери за такива инструменти са тези, които поразяват софтуера за защита на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Без одобрение на прекия ръководител или по-горестоящ, е забранено използването на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или оперирящ компютър. Неоторизирано използване на такива инструменти може да доведе до дисциплинарни наказания;

- При внедряване на нов програмен продукт, свързан с обработване на лични данни, следва да предварително да се оценят възможностите му, с оглед спазване изискванията на защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване;

- При необходимост от ремонт на компютърната техника, предоставянето ѝ на външна сервизна организация да се извършва без устройствата, на които се съхраняват лични данни;

4.8. Копия/резервни копия за възстановяване;

- Целта на Администратора е да поддържа информацията налична. Информацията, съдържаща лични данни трябва да бъде архивирана в съответствие със стандартите за архивиране на данни. За мулти-потребителски компютърни и комуникационни системи, системният администратор е отговорен за извършване на периодични архивирания. Ако бъде поискано, IT- специалистите на Университета трябва да инсталират или предоставят техническа помощ за инсталирането на резервен хардуер.

- Всички архиви, съдържащи поверителна и/или служебна информация трябва да се съхраняват с физически контрол на достъпа и трябва да се инвентаризират периодично;

4.9. Физическа среда/обкръжение;

- Администраторът осъществява физически контрол включително заключени врати, поддържане на подходяща температура и нива на влажност и наличието на пожарогасителната система са осигурени за защита на IT- оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване;

4.10. Персонална защита;

- Осигурени са охранителни услуги в помещенията за защита на физическата среда от нарушители, включително жива охрана и охрана с технически средства 24 часа в денонощието;

4.11. Процедури за унищожаване/заличаване/изтриване на носители:

- Данни, които вече не са необходими за правно-регламентирани цели, трябва да бъдат унищожени по безопасен начин чрез средства, като нарязване, изгаряне или постоянно заличаване от електронните средства. Когато трета страна е ангажирана да провежда безопасни процеси по унищожаване от името на Администратора на лични данни, трябва да се изиска протокол за извършено унищожаване на лични данни;

4.12. План при извънредни ситуации:

Администраторът трябва да има резервен план за възстановяване при извънредна ситуация, който се разработва, поддържа и изпълнява от оторизираните IT-специалисти. Планът за възстановяване при извънредни ситуации се поддържа за приложения, които боравят с важна информация, включително съдържаща лични данни, за да се осигури наличието на тази информация. IT- специалистите трябва да съгласуват с ДЛЗД и ръководителите на основни звена кои данни се включват в плана за възстановяване след извънредна ситуация. Отговорност на IT- специалистите е изпълнението на плана за действие в извънредни ситуации в случай на отказ на системата. В случай на извънредна ситуация, засягаща сигурността на личните данни, незабавно се уведомява ДЛЗД. Планът за действие в извънредни ситуации трябва да бъде адекватно развит, да се актуализира редовно и да се проверява периодично.

5. Крипторафска защита.

Допустими криптиращи технологии за операционните системи на Университета, системите за управление на бази-данни и комуникационното оборудване трябва да бъдат стандартните такива, включително симетрично криптиращите технологии. Криптирането се използва за защита на личните данни, които се предават от Администратора на лични данни по електронен път или на преносими носители, когато такива данни се предават извън логическия или физическия контрол на Университета.

## XVI. ПОЛУЧАТЕЛИ, НА КОИТО МОГАТ ДА БЪДАТ РАЗКРИТИ ЛИЧНИТЕ ДАННИ

Администраторът ще събира, обработва и използва предоставените от Вас лични данни само за целите, за които Субектите са били уведомени. Те няма да бъдат разкривани на трети страни, без Вашето изрично съгласие. Администраторът има право да разкрива обработваните лични данни: на Субектите, за които се отнасят данните; на лица, ако е предвидено в нормативен акт и на лица, обработващи личните данни. При наличието на законово задължение Администраторът има право и без съгласието на Субекта да предостави определена информация на органите на съдебната власт, доброволен арбитраж, медиатори, адвокати, нотариуси, съдебни изпълнители, агенции за събиране на вземания, финансови институции, държавни органи, или на правоприлагащи органи за предотвратяване на потенциални нарушения или противоправно поведение. Администраторът има право да разкрие информация и когато това му е било поискано по съдебен ред или по друг законов начин, или с цел изясняване на факти по съдебен спор или предотвратяване на евентуално увреждане на лица или имущество. Във всички случаи преди да предостави данните на трето лице Администраторът проверява дали е налице правно основание за това и преценява обема на данните, който следва да предостави. Предоставянето на лични данни на трети лица или употребата им надхвърляща нуждите конкретно полученото запитване или искане не се допуска. Служителите са обучени и инструктирани, че всички случаи на предоставяне на лични данни от Администратора на трети лица се документират.

## XVII. ПРАВА НА СУБЕКТИТЕ НА ДАННИТЕ

Субектът, чиито лични данни се обработват има следните права:

- Право на достъп до отнасящите се за него данни;

- Право на коригиране;

- Право на изтриване (право „да бъдеш забравен“), изразяващо се в правото да поиска от Администратора изтриване на свързаните с него лични данни без ненужно забавяне, а Администраторът има задължение да го изтрие при наличието на определени предпоставки, като: личните данни не са повече необходими за целите, за които са били събрани; субектът на данните е оттеглил съгласието си; субектът на данните е направил възражение съгласно чл.21, пар.1 от Общия Регламент за защита на данните 2016/679- GDPR и няма законни основания за обработването; личните данни са били обработвани незаконосъобразно; личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава-членка; личните данни са били събрани във връзка с предлагането на услуги на информационнното общество;

- Право на ограничаване на обработването, което може да се упражни в следните случаи: когато точността на данните се оспорва от Субекта; когато обработването е неправомерно, но Субектът не желае данните да бъдат изтрити, а само иска да ограничи използването им; когато Администраторът не се нуждае повече от личните данни, но Субектът ги изисква във връзка с упражняването и защитата на негови правни претенции; когато Субектът е възразил срещу обработването и е в очакване на проверката дали основанията на Администратора имат предимство пред неговите интереси;

- Право на преносимост на данните- Субектът има право да получи личните данни, които го засягат и които той е предоставил на Университета в структуриран и пригоден за машинно четене формат[2]. Субектът има правото да прехвърли тези данни на друг администратор без възпрепятстване от Администратора, на когото личните данни са предоставени, когато: обработването е основано на съгласие или се извършва по автоматизиран начин.

- Право на уведомяване за нарушение на сигурността на личните данни;

- Право на защита по съдебен и административен ред (право на подаване на жалба до надзорен орган; право на ефективна съдебна защита срещу надзорен орган; право на ефективна съдебна защита срещу администратор или обработващ лични данни);

- Право на обезщетение за претърпени вреди;

- Право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласието, което е дадено, преди то да бъде оттеглено.

Субектът има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, в случаите, в които обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора или обработването е необходимо за целите на легитимните интереси на Администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на потребителя, които изискват защита на личните данни, по-специално когато потребителят е дете.

## XVIII. РЕД ЗА УПРАЖНЯВАНЕ НА ПРАВАТА

Субектите упражняват правата си, включително правото на достъп, правото на изтриване, коригиране или ограничаване на обработването чрез подаването на писмено искане до Администратора. Администраторът предоставя на Субекта информация относно действията, предприети във връзка с искането, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира Субекта за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато Субектът е подал искането с електронни средства, по възможност информацията му се предоставя с електронни средства, освен ако Субектът не е поискал друго. Ако Администраторът не предприеме действия по искането на Субекта, Администраторът уведомява Субекта без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорния орган и търсене на защита по съдебен ред.

[2] Машинно-читаем формат е формат, който позволява компютърна програма еднозначно и надеждно да идентифицира съдържащите се в електронния документ електронни данни, както и вътрешната им структура.

## XIX. ИНФОРМАЦИЯ ОТНОСНО ИЗВЪРШВАНЕТО НА ПРОФИЛИРАНЕ И ЗА ПОСЛЕДСТВИЯТА ОТ ТОВА ПРОФИЛИРАНЕ:

Администраторът не извършва профилиране. „Профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение. Субектът има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което да породи правни последици за субекта на данните, или по подобен начин да го засегне в значителна степен. Изключения от това право са случаите, когато решението е необходимо за сключването или изпълнението на договор, когато е разрешено по закон, когато се основава на изричното съгласие на Субекта на данни.

## XX. ПРОМЕНИ В ПОЛИТИКАТА ЗА ПОВЕРИТЕЛНОСТ

Администраторът има право да изменя и допълва Политиката за защита на личните данни по всяко време. Актуализираната политика за поверителност влиза в сила от датата, на която е публикувана на уебсайта или оповестена по друг подходящ начин.

Настоящата Политика за поверителност влиза в сила на 25.05.2018 година.