ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ НА ВИСШЕТО УЧИЛИЩЕ ПО ТЕЛЕКОМУНИКАЦИИ И ПОЩИ

София 2018

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита.

(2) Настоящите правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).

(3) Правилата се утвърждават, допълват, изменят и отменят от Ректора на Висшето училище по телекомуникации и пощи– администратор на лични данни.

(4) Висшето училище по телекомуникации и пощи предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

II. ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

Чл. 2. Настоящите Правила имат за цел да регламентират:

(1) механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;

(2) задълженията на Висшето училище по телекомуникации и пощи като администратор на лични данни, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;

(3) правилата за разпределение на личните данни и групирането им в регистри и Правилата за работа с личните данни;

(4) необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

Чл. 3. Правилата са задължителни за всички лица имащи достъп до личните данни, обработвани за нуждите на Висшето училище по телекомуникации и пощи.

III. ПРЕДНАЗНАЧЕНИЕ И ВИДОВЕ РЕГИСТРИ

Регистри. Видове.

Чл. 4. (1) В изпълнение на дейностите си Висшето училище по телекомуникации и пощи поддържа следните регистри на лични данни:

а. Регистър „Счетоводство“

б. Регистър „Административен отдел“

в. Регистър „Видео наблюдение и пропусквателен режим“

г. Регистър „Учебен отдел“

д. Регистър „Студентски общежития“

е. Регистър „Финансов контрол“

(2) Регистрите набират и съхраняват лични данни на студентите, академичния състав и непреподавателския персонал с оглед:

1. индивидуализиране на лицата, чиито данни подлежат на обработка;

2. изпълнение на нормативните изисквания за защита от неправомерно използване на лични данни на горепосочените лица;

3. използване на събраните данни за съответните лица само за служебни цели;

4. установяване при възникнала необходимост на връзка с лицата, изпращане на кореспонденция, отнасяща се до техни права и законни интереси.

(3) Създаването на нови регистри и извършването на промени се извършва със заповед на Ректора.

Форми на водене на регистъра

Чл. 5. (1) Формите на водене на регистрите биват на хартиен и технически (магнитен) носител.

1. Водене на регистър на хартиен носител:

1.1. Форма на организация и съхраняване на личните данни – писмена (документална);

1.2. Местонахождение на картотечния шкаф – в офиса на обработващите личните данни в отделите;

(2) Носител (форма) за предоставяне на данните от физическите лица – личните данни от лицата се подават на Висшето училище по телекомуникации и пощи и оправомощеното лице, назначено за обработването им – обработващ лични данни, на основание нормативно задължение във всички случаи, когато е необходимо;

1. Достъп до личните данни – такъв има само обработващият лични данни.

(3) Водене на регистър на технически (магнитен) носител:

1. Форма на организация и съхраняване на личните данни – личните данни се съхраняват на твърд диск, на изолиран компютър;

2. Местонахождение на компютъра – в офиса на обработващ личните данни в съответния отдел;

3. Достъп до личните данни и защита - достъп до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове, както и длъжностното лице по защита на личните данни посредством делегирани му права и задължения от Ректора на Висшето училище по телекомуникации и пощи.

Групи данни в регистъра

Чл. 6. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:

1. физическата идентичност на лицата – имена, ЕГН, номер на документ за

самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт;

2. семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;

3. образование – вид на образованието, място, номер и дата на издаването на дипломата, научни степени, научни звания, публикации, допълнителна квалификация и др.;

4. трудова дейност – професионална биография, дни в осигуряване, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;

5. медицински данни – здраве статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;

6. други лични данни – осигурителен доход, трудови възнаграждения, парични обезщетения, статус на лицето (осъждано/неосъждано/реабилитирано) и други.

(2) Личните данни в регистрите се събират от Висшето училище по телекомуникации и пощи на хартиен или електронен носител.

Задължения на лицето, отговарящо за водене и съхраняване на данните в регистрите

Чл. 7. Задълженията на лицето, отговарящо за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

Периодично архивиране

Чл. 8. Архивиране на личните данни на технически носител се извършва периодично на всеки шест месеца регулярно за цялата база лични данни и след приключването на всяко по-голямо събиране на лични данни, като Кандидатстудентска кампания, Прием на студенти, Дипломиране на випуск за съответно събраните лични данни от посочената дейност. Архивирането се извършва от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

Контрол при обработване на личните данни

Чл. 9. (1) Контролът върху дейностите по обработка на лични данни се осъществява от длъжностното лице по защита на данните.

(2) За целта Висшето училище по телекомуникации и пощи назначава нарочен служител като длъжностно лице по защита на данните.

Актуализация на лични данни

Чл. 10. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в училището. Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице промяна, грешка или непълнота в тях, и удостовери това с документ;

2. по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;

3. при установена грешка при обработката на личните данни от страна на Обработващ личните данни;

(2) При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето, обработващо личните данни.

IV. ДОСТЪП ДО ЛИЧНИ ДАННИ И ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Лица с право на достъп

Чл. 11. (1) Всяко физическо лице, включително академичния състав и служителите, има право на достъп до отнасящите се до него лични данни, обработвани от Висшето училище по телекомуникации и пощи.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, Висшето училище по телекомуникации и пощи предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се него.

(3) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от Висшето училище по телекомуникации и пощи:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Осъществяване правото на достъп

Чл. 12. (1) Правото на достъп се осъществява с писмена молба до Ректора на Висшето училище по телекомуникации и пощи.

(2) Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Молбата по ал. 1 се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Чл. 13. (1) Молбата по чл. 12 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;

2. описание на искането;

4. предпочитана форма за предоставяне на достъп до личните данни;

5. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на молба от упълномощено лице към същото се прилага и

нотариално завереното пълномощно.

(3) При приемане на молбата, техническо лице извършва регистрация на същата в деловодната система на Висшето училище по телекомуникации и пощи.

Чл. 14. (1) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Висшето училище по телекомуникации и пощи е длъжно да се съобрази с предпочитаната от молителя форма на предоставяне на информацията по чл. 11, ал. 3.

(3) Висшето училище по телекомуникации и пощи предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;

2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Разрешаване достъпа и предоставяне на информация

Чл. 15. (1) Ректорът на Висшето училище по телекомуникации и пощи или изрично оправомощено от него лице разглежда молбата по чл. 11 и се произнася в 14-дневен срок от неговото постъпване с решение. Обработващите лични данни предоставят необходимите данни на оправомощеното от Ректора лице.

(2) Срокът по ал. 1 може да бъде удължен от Ректора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на Висшето училище по телекомуникации и пощи.

(3) С решението си Ректорът на Висшето училище по телекомуникации и пощи или изрично оправомощено от него лице предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето й.

Чл. 16. Право на достъп до данните в поддържаните от Висшето училище по телекомуникации и пощи регистри на лични данни имат служителите в училището –администратори на базите данни, служителите на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни), както и служителите, за които служебните им функции налагат такъв достъп.

Чл. 17. Служителите във Висшето училище с оторизиран достъп до лични данни са длъжни да обработват същите законосъобразно и добросъвестно, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги поддържат във вид, който им позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които се обработват.

V. ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ, СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 18. (1) Достъп до обработваните от Висшето училище по телекомуникации и пощи лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на Висшето училище.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице Висшето училище по телекомуникации и пощи съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

VI. ВИДОВЕ ЗАЩИТА НА ЛИЧНИ ДАННИ

Длъжностно лице по защита на личните данни

Чл. 19. (1) За обезпечаване на адекватна защита на регистрите с лични данни Висшето училище по телекомуникации и пощи определя и/или назначава лице/лица по защита на личните данни.

(2) Лицето/лицата по защита на личните данни има следните правомощия:

1. осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;

2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;

3. осъществява контрол по спазване на изискванията по защита на регистрите;

4. специфицира техническите ресурси, прилагани за обработване на личните данни;

5. подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;

6. в случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък **Ректора на** Висшето училище по телекомуникации и пощи. Настъпилото събитие поражда задължение за Висшето училище по телекомуникации и пощи в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни;

7. поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;

8. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

9. периодично информира персонала по въпросите на защитата на личните данни;

10. следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Видове защита на личните данни

Чл. 20. (1) С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, Висшето училище по телекомуникации и пощи организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) Видове защита:

1. Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

2. Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на Ректора на Висшето училище по телекомуникации и пощи.

3. Документална защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.

4. Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

5. Псевдонимизация1 чрез употребата на технически и организационни мерки.

6. Мерките на различните видове защита се определят съгласно приложение № 6 от настоящите Правила.

Предоставяне на документи, съдържащи лични данни

Чл. 21 (1) Всяко лице желаещо да внесе документ съдържащ лични данни предоставя същия в деловодството на Висшето училище по телекомуникации и пощи. Лицето приемащо документа е задължено да запознае вносителят на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му, вносителят попълва съответна Декларация по образец предоставена му от лицето приемащо документите за деклариране на предоставените лични данни и основанието, на което те се предоставят и ще се ползват. Лицето, приемащо документите има право да изиска от субекта на лични данни документа, доказващ истинността на предоставените лични данни, а при наличие на предвидена в закона възможност, да снима копие от този документ и да го приложи към декларацията.

(2) Внесените документи с лични данни се докладват на Ректора или определено от него лице, който ги разпределя на лицата обработващи съответните лични данни.

(3) Лицата обработващи личните данни са задължени да предоставят личните данни в съответствие с разпореждането на Ректора.

(4) Лични данни се предоставят на трети лица само чрез Ректора или определено от него лице.

(5) При предоставяне на личните данни за ползване от трети лица, те попълват декларация за задължението си да обработват личните данни съгласно Регламент 2016/679 и ЗЗЛд.

VII. МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Правила за защита

Чл. 22. (1) Правилата за защита при обработване на лични данни регламентират технически мерки, които:

1. отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;

2. предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;

3. предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;

4. предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;

5. гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;

6. осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;

7. осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;

8. предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;

9. осигуряване на възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;

10. осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

Мерки за защита

Чл. 23. (1) Служителят/ите, обработващ/и лични данни, взема/т мерки за гарантиране на надеждност при обработването, като осъществява/т технически и организационни мерки за защита на личните данни.

(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:

1. неоторизирано четене, възпроизвеждане, промяна или премахване на носителя на данните;

2. неоторизирано въвеждане, промяна или заличаване на съхранени лични данни;

3. неоторизирано използване на системите за лични данни чрез средства за пренос на данни;

4. неоторизиран достъп до лични данни.

VIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл. 24. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

(2) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 25. При оценката на въздействието Висшето училище по телекомуникации и пощи отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.

2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели,

или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;

3. лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;

4. лични данни в широкомащабни регистри на лични данни;

5. данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

IX. НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 26. Определят се следните нива на въздействие:

1. „Изключително високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. „Високо” – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. „Средно” – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. „Ниско” – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 27. (1) Висшето училище по телекомуникации и пощи извършва оценка на въздействие за всички поддържани регистри .

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2, определя нивото на въздействие на съответния регистър.

Чл. 28. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 29. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) Нивата на защита са, както следва:

1. при ниско ниво на въздействие – ниско ниво на защита;

2. при средно ниво на въздействие – средно ниво на защита;

3. при високо ниво на въздействие – високо ниво на защита;

4. при изключително високо ниво на въздействие – изключително високо ниво на защита.

X. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ ПРИ ИНЦИДЕНТИ

Чл. 30. (1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на лицето по защита на личните данни във Висшето училище по телекомуникации и пощи.

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

(3) След анализ от лицето по защита на личните данни, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

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

(5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

XI. ОТГОВОРНОСТ

Чл. 31. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание, ако такава отговорност се предвижда по закон.

Чл. 32. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители във Висшето училище по телекомуникации пощи, засегнатите лица могат да търсят отговорност от

виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на Висшето училище по телекомуникации и пощи на виновните лица се търси имуществена отговорност по Кодекса на труда.

XII. ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Дефиниции

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

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

3. „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;

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

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

6. „надзорен орган" означава независим публичен орган, създаден от държава членка и отговорен за наблюдението на прилагането на Регламент (ЕС) 2016/679. В Република България това е Комисията за защита на личните данни, чиито контактни данни ще намерите по-долу.

§2. За целите на този правилник:

1. "Администратор на лични данни" е Висшето училище по телекомуникации и пощи – София;

2. "Длъжностно лице защита на данни" е специалист „Сигурност“ във Висшето училище по телекомуникации и пощи.

3. "Обработващ лични данни" са физическите лица, ръководители и служители в отделите: Финасово-счетоводен, Административен отдел, Учебен отдел, Студентски общежития, Видеонаблюдение и пропускателен режим, Финансов контрольор.

§ 3. Настоящите Вътрешни правила се издава на основание чл. 24, ал. 4 от Закона за защита на личните данни.

§4. За всички неуредени случаи се прилагат разпоредбите на Регламент 2016/679, ЗЗЛД и разпорежданията на ЗЗЛд.

§5. Вътрешните правила влизат в сила в деня на тяхното утвърждаване от Ректора на Висшето училище по телекомуникации и пощи – 20.08.2018 година.

§6. Екземпляр от Вътрешните правила да се предоставят на Административен отдел за сведение и изпълнение.

Настоящите правила са утвърдени от Ректора на Висшето училище по телекомуникации и пощи.