ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ

“ГЕОРГИ БЕНКОВСКИ“

Изх. рег. № / .06.2020 г.

Екз. единствен

ВЪТРЕШНИ ПРАВИЛА

ЗА СЪБИРАНЕ, ОБРАБОТВАНЕ И СЪХРАНЕНИЕ НА

ЛИЧНИ ДАННИ ВЪВ ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ „ГЕОРГИ БЕНКОВСКИ”

Долна Митрополия

2020

ВЪТРЕШНИ ПРАВИЛА
ЗА СЪБИРАНЕ, ОБРАБОТВАНЕ И СЪХРАНЕНИЕ НА ЛИЧНИ ДАННИ ВЪВ ВВВУ „ГЕОРГИ БЕНКОВСКИ ”

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите вътрешни правила се прилагат за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни, или които са предназначени да съставляват част от регистър с лични данни и имат за цел да регламентират:

(1) воденето, поддържането и защитата на регистри, съхраняващи лични данни на физическите лица във ВВВУ „Георги Бенковски” – гр. Долна Митрополия;

(2) задълженията на длъжностните лица, обработващи лични данни и тяхната отговорност при неизпълнение на тези задължения;

(3) необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, 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. 2. (1) Обработването на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп, като се спазва принципа „необходимост да се знае“.

Чл. 3. Определения:

(1) **„Лични данни”** - 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) **„Специални категории лични данни”** – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.

(3) **„Обработване”** - 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;

(4) **„Ограничаване на обработването”** - маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

(5) **„Регистър с лични данни”** - 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;

(6) **„Администратор”** - 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;

(7) **„Субект на данните”** – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.

(8) **„Съгласие на субекта на данните”** - 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;

(9) **„Профилиране”** - 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;

(10) **„Обработващ лични данни”** - физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

(11) **„Получател”** - 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;

(12) **„Нарушение на сигурността на лични данни”** - 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;

(13) **„Трета страна”** – всяко 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;

(14) **„Данни за здравословното състояние”** - лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

(15) **„Задължителни фирмени правила”** - политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка.

(16) **„Цялостност”** - изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

(17) **„Поверителност”** - изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

(18) **„Надзорен орган”** - независим публичен орган, създаден от държава членка съгласно член 51 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета. За България това е Комисията за защита на личните данни.

ПРИНЦИПИ, СВЪРЗАНИ С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл. 4. Личните данни трябва да бъдат:

(1) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните:

1. **Законосъобразно** – да идентифицира законна основа, преди да може да обработва лични данни. Те често са посочени като „основания за обработване", например „съгласие“.

2. **Добросъвестно** - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

3. **Прозрачно** – Общият регламент включва правила относно предоставяне на поверителна информация на субектите на данни. Те са подробни и конкретни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

(2) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели („ограничение на целите”);

(3) адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел (принцип на минимално необходимото);

(4) точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност”);

(5) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват

за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1 от Регламент (ЕС) 2016/679, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в Регламент (ЕС) 2016/679 с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението”);

(6) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност”);

(7) администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни („отчетност”).

ЗАКОНОСЪОБРАЗНОСТ НА ОБРАБОТВАНЕТО

Чл. 5. (1) Обработването е законосъобразно, когато:

1. субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

2. обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

3. обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

4. обработването е необходимо за изпълнение на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

Чл. 6. (1) Когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на съгласието на субекта на данните или на правото на Съюза или правото на държава членка, администраторът, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, взема под внимание:

1. всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;

2. контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и

администратора;

3. възможните последствия от предвиденото по-нататъшно обработване за субектите на данните.

ДАВАНЕ НА СЪГЛАСИЕ

Чл. 7. (1) Под „съгласие” ВВВУ ще разбира 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. Субектът на данните може да оттегли своето съгласие по всяко време.

(2) Така също под „съгласие” ВВВУ разбира само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

Чл. 8. Условия за даване на съгласие:

1. Когато обработването се извършва въз основа на съгласие, администраторът трябва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни.

2. Ако съгласието на субекта на данните е дадено в рамките на писмена декларация (Приложение 1), която се отнася и до други въпроси, искането за съгласие се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като използва ясен и прост език.

3. Субектът на данни има правото да оттегли съгласието си по всяко време като за целта попълва заявление за оттегляне на съгласие (Приложение 2). Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това.

ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 9. Забранява се обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за

здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, освен ако:

1. субектът на данни е дал своето изрично съгласие за обработването на тези лични данни;

2. обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила;

3. обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

4. обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи.

ПРАВА НА СУБЕКТА НА ДАННИ

Чл. 10. Субектите на данни имат следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

1. да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;

2. да поиска копие от своите лични данни от администратора;

3. да иска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;

4. да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");

5. да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани;

6. да направи възражение срещу обработване на негови лични данни;

7. да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг;

8. да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на ОРЗД е нарушена;

9. да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;

10. да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;

11. да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;

12. да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

Чл. 11. (1) ВВВУ „Г. Бенковски" (Администраторът) предприема необходимите мерки за предоставяне на информация, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език. Информацията се предоставя след подаване от лицето на заявление за достъп до личните си данни (Приложение 3). Поисканата информация се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства.

(2) ВВВУ „Г. Бенковски" (Администраторът) съдейства за упражняването на правата на субекта на данните, освен ако докаже, че не е в състояние да идентифицира субекта на данните.

ПРЕДОСТАВЯНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 12. (1) Лицата имат право на достъп до личните си данни, за което лично подават заявление до началника на ВВВУ „Г. Бенковски". Подаването на заявление е безплатно.

(2) Заявлението съдържа - име, адрес и други данни идентифициращи съответното физическо лице; описание на искането; предпочитана форма за предоставяне на информацията; подпис, дата на подаване на заявлението и адрес за кореспонденция, в случай, ако субекта не желае да получи информацията на място.

(3) Заявлението се завежда в Регистратура за некласифицирана информация.

(4) Личните данни се предоставят само на лицата, за които се отнасят.

Чл. 13. (1) Срокът за разглеждане на заявлението и произнасянето по него е 30-дневен от деня на постъпване в Училището.

(2) Решението се съобщава на заявителя, получава се лично срещу подпис или по пощата с обратна разписка.

(3) ВВВУ „Г. Бенковски" като администратор може да откаже предоставяне на информация в случаи на неоснователност или когато вече е предоставяна такава информация на субекта.

Чл. 14. Достъп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на копие от исканата информация.

Чл. 15. ВВВУ „Г. Бенковски" като администратор на лични данни има право да предостави лични данни на институции, за които правото на достъп е предвидено в нормативен акт.

СИГУРНОСТ НА ДАННИТЕ

Чл. 16. ВВВУ „Г. Бенковски" прилага адекватна защита на личните данни, която включва:

1. физическа защита;
2. персонална защита;
3. документална защита;
4. защита на автоматизирани информационни системи и мрежи;
5. Криптографска защита.

Чл. 17. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на ВВВУ и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на ВВВУ се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения,

съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 18. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от ВВВУ, подписват декларация за съгласие по образец (Приложение № 1).

Чл. 19. (1) Всички служители, които обработват и/или съхраняват лични данни са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които ВВВУ съхранява, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако ВВВУ не е дал такива права на тази трета страна, като са сключили договор/клауза за поверителност .

(2) Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

1. в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека;

2. ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (*например правила за контрол на достъпа*);

3. съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

(3) Компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители на ВВВУ. От всички служители които обработват и/или съхраняват лични данни се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

(4) Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за

текущата работа по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.

(5) Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данните. Записите на хартиен носител, които са достигнали крайната дата на съхранение, трябва да бъдат нарязани и унищожени. Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури.

(6) Обработването на лични данни „извън ВВВУ" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 20. ***Физическата защита*** в ВВВУ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 21. (1) Основните ***организационни мерки за физическа защита*** във ВВВУ включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
3. определяне на организацията на физическия достъп.

(2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична" част, в която се извършват дейностите по

обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове*, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(4) *Организацията на физическия достъп до помещения*, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(5) *Зони с контролиран достъп* са всички помещения на територията на ВВВУ, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни във ВВВУ са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

(8) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

Чл. 22. (1). Основните ***технически мерки за физическа защита*** във ВВВУ включват:

1. използване на ключалки и заключващи механизми;
2. шкафове, метални каси;
3. оборудване на помещенията с пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки, които могат да се заключват*, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: *ключалки* (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(4) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 23. (1). Основните ***мерки за персонална защита*** на личните данни, приложими във ВВВУ, са:

1. задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (Приложение № 4);
2. запознаване и осъзнаване за опасностите за личните данни, обработвани от ВВВУ;
3. забрана за споделяне на критична информация (идентификатори, пароли за достъп и др. подобни) между персонала и всякакви други лица, които са неоторизирани;
4. деклариране на съгласие за поемане на задължение за неразпространение на личните данни (Приложение № 5);

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните

задължения изисква подобно.

Чл. 24. (1) Основните ***мерки за документална защита*** на личните данни, са:

1. *определяне на регистрите, които ще се поддържат на хартиен носител* - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на ВВВУ, като кандидат студентска кампания, кандидат курсантска кампания, сключване на договори, изпълнение на договори, обучение на курсанти, студенти и кадети, упражняване на предвидени в закона права и установени от закона задължения и др.;

2. *определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на ВВВУ, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

3. *регламентиране на достъпа до регистрите с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;

4. *определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.

(2) *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на ВВВУ или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;

2. *Правила за размножаване и разпространение*, които разрешават

копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл. 25. (1) ***Защитата на автоматизираните информационни системи и/или мрежи*** във ВВВУ включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на ВВВУ. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае”;

2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;

3. Управление на *външни връзки и/или свързване*, включващо от своя страна:

а) Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка”, които се намират под контрола и администрацията на ВВВУ. Като *външни мрежи* се разглеждат всички мрежи, вкл. и 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 ВВВУ;

б) Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от Началника на ВВВУ лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае”. Минимално изискваното ниво на сигурност за достъп до вътрешните

мрежи изисква идентифициране с уникално потребителско име и парола.

в) Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

г) Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на ВВВУ, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. *Защитата от зловреден софтуер* включва:

а) използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от Ръководството на ВВВУ лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалистите на ВВВУ.

б) използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Ръководството на ВВВУ лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

в) активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

г) забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от Ръководството на ВВВУ лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

а) Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на ВВВУ.

б) Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

в) Отговорност за архивиране има лицето, обработващо личните данни.

г) Срокът на архивиране следва да е съобразен с действащото законодателство.

д) Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

е) Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)

ж) *Персоналната защита на данните* е част от цялостната охрана на ВВВУ.

з) *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на ВВВУ.

и) Данните, които вече не са необходими за целите на ВВВУ и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. *Организация на телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на ВВВУ:

а) Отдалечен достъп до вътрешни мрежи на ВВВУ не е предвиден. По изключение, и след изричната оторизация от Ръководството на ВВВУ, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

б) На персонала на ВВВУ може да бъде предоставен интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано с оторизираните от Ръководството на ВВВУ лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от Ръководството на ВВВУ и след становище на длъжностното лице по защита на данните. Отдалечен достъп чрез интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ВВВУ както и в случаите на заплаха за сигурността на данните.

в) Публикуването на служебна информация в интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Ръководството на ВВВУ.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на ВВВУ, включват:

а) Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на ВВВУ от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

б) Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на ВВВУ, които биха могли да бъдат използвани,за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

в) Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими

способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл. 26. (1) По отношение на личните данни се прилагат и мерки, свързани с ***криптографска защита на данните*** чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

(2) Криптирането се използва и за защита на личните данни, които се предават от ВВВУ по електронен път или на преносими носители.

БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 27. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) ВВВУ прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 300 секунди), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от ВВВУ период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, не изключване на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Ръководството и Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 28. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 29. (1) Във ВВВУ се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от Ръководството на ВВВУ лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 30. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

РАЗКРИВАНЕ НА ДАННИ

Чл. 31. (1) ВВВУ трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички

служители/работници трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността извършвана от организацията.

(2) Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Длъжностното лице за защита на данните.

СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 32. (1) ВВВУ не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

(2) ВВВУ може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

(3) Периода на съхранение за всяка категория на лични данни са изложени в процедурата за съхраняване и унищожаване на данните, както и на критериите, използвани за определяне на този период, включително всякакви законови задължения.

(4) Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1, б. е от Общия регламент), включително защитата срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност”).

УВЕДОМЯВАНЕ НА НАДЗОРНИЯ ОРГАН И СЪОБЩАВАНЕ НА СУБЕКТА НА ДАННИТЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 33. (1) Съгласно чл. 33 от ОРЗД в случай на нарушение на сигурността на личните данни ВВВУ „Г. Бенковски” като администратор, без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган, като длъжностното лице по защита на личните данни изпраща уведомително писмо (Приложение 6) до

надзорният орган компетентен в съответствие с чл. 55 от ОРЗД, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(2) Обработващият лични данни уведомява администратора и длъжностното лице по защита на данните без ненужно забавяне, след като узнае за нарушаване на сигурността на личните данни като попълва уведомление до администратора (Приложение 7).

(3) Уведомлението трябва да съдържа най-малко следното:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. посочване на името и координатите за връзка на длъжностното лице по защита на данните или друга точка за контакт, от която може да се получи повече информация;

3. описание на евентуалните последици от нарушаването на сигурността на личните данни;

4. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

(5) Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

Чл. 34. (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, уведомява субекта на данните за нарушението на сигурността на личните данни с писмо (Приложение 8), но не по-късно от 7 дни от установяването му.

(2) В съобщението до субекта на данните на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най- малко информацията и мерките, посочени в чл. 33, ал. 3, т. 2 - 4.

(3) Съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

1. предприети са подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2. взети са мерки, които гарантират, че вече няма вероятност да се материализира високия риск за правата и свободите на субектите на данни;

3. то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

(4) Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, надзорният орган може, след като отчете каква е вероятността от нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да уведоми субекта на данните.

ЗАДЪЛЖЕНИЯ И ОТГОВОРНОСТИ

Длъжностно лице по защита на данните

Чл. 35. (1) Съгласно заповед на началника на ВВВУ „Г. Бенковски" и в изпълнение на чл. 37 от ОРЗД е определено длъжностно лице по защита на личните данни във ВВВУ „Г. Бенковски".

(2) Длъжностното лице по защита на данните има следните задачи:

1. да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Регламент (ЕС) 2016/679 и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

2. да наблюдава спазването на Регламент (ЕС) 2016/679 и на други разпоредби за защитата на данни на равнище Съюз или държава членка и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на служителите, участващи в операциите по обработване, и съответните одити;

3. при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно чл. 35 от Регламент (ЕС) 2016/679;

4. да си сътрудничи с надзорния орган;

5. да действа като звено за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителна консултация, посочена в чл. 36 от Регламент (ЕС) 2016/679, и по целесъобразност да се консултира по всякакви други въпроси.

(3) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработване.

(4) Длъжностното лице по защита на данните е натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на Регламент (ЕС) 2016/679 в организацията на администратора и повишаването на осведомеността и обучението на персонала.

(5) В чл. 38 от Регламент (ЕС) 2016/679 са предвидени основните елементи от правното положение на длъжностното лице по защита на данните. Те са предпоставка за ефективното изпълнение на неговите задачи и очертават статута, който той има в организацията на администратора или обработващия.

Служители на ВВВУ „Г. Бенковски”, действащи под ръководството на администратора на лични данни

Чл. 36. Служителите на ВВВУ, действащи под ръководството на администратора на лични данни са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират при необходимост регистрите на личните данни;

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;

6. да спазват нормативната уредба в областта на защитата на личните данни.

Администратор и външна организация, обработваща лични данни от името на администратора

Чл. 37. (1) Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламент (ЕС) 2016/679. При необходимост тези мерки се актуализират.

(2) ВВВУ „Г. Бенковски" като администратор осигурява спазването на принципите, свързани с обработването на лични данни.

(3) ВВВУ „Г. Бенковски" като администратор на лични данни обработва личните данни самостоятелно или чрез възлагане на обработващ лични данни.

Чл. 38. Задължения за администратора и външната организация обработваща лични данни от името на администратора:

1. Обработване на данните в съответствие с принципите за защита на личните данни, заложени в Регламент (ЕС) 2016/679, като е в състояние да докаже това (отчетност);
2. Осигуряване защита на данните;
3. Поддържане на регистър на дейностите по обработване, за които отговаря;
4. Уведомяване на надзорния орган и субекта на данни в случай на нарушаване на сигурността на личните данни, както и документиране на всяко нарушение на сигурността на личните данни, в т.ч. фактите, свързани с нарушението, последиците от него, предприетите действия за справяне с нарушението;
5. Извършване на оценка на въздействието върху защитата на данните;
6. Провеждане на предварителна консултация с надзорния орган преди обработването, когато оценката на въздействието покаже, че обработването ще породи висок риск, ако администратора не предприеме мерки за ограничаване на риска;
7. Прилагане на подходящи технически и организационни мерки за осигуряване на сигурност на данните.

Чл. 39. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ВВВУ „Г. Бенковски" или за трето

лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

Чл. 40. Обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение, обработващият данни винаги информира администратора за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като по този начин даде възможност на администратора да оспори тези промени.

Чл. 41. (1) Обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора, и който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора. В договора или друг правен акт се предвижда по-специално, че обработващият лични данни:

1. обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;

2. гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

3. взема всички необходими мерки съгласно член 32 от Регламент (ЕС) 2016/679;

4. спазва условията по чл. 41 и чл. 42 за включване на друг обработващ лични данни;

5. като взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените права на субектите на данни;

6. подпомага администратора да гарантира изпълнението на задълженията съгласно членове 32—36 от Регламент (ЕС) 2016/679, като отчита естеството на обработване и информацията, до която е осигурен достъп

на обработващия лични данни;

7. по избор на администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка не изисква тяхното съхранение;

8. осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора.

(2) Предвид точка 8 от първа алинея обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава Регламент (ЕС) 2016/679 или други разпоредби на Съюза или на държавите членки относно защитата на данни.

Чл. 42. Когато обработващ лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на администратора, чрез договор или друг правен акт съгласно правото на Съюза или правото на държава членка на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни, както е посочено в чл. 41, по-специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията на Регламент (ЕС) 2016/679. Когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този друг обработващ лични данни.

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Чл. 43. В регистъра се събират, обработват и съхраняват лични данни на физически лица с оглед:

1. Индивидуализиране на лицата, чиито данни подлежат на обработка.

2. Използване на събраните данни за съответните лица само за служебни цели.

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

Чл. 44. (1) ВВВУ „Г. Бенковски” като администратор поддържа

регистър на дейностите по обработване, за които отговоря. Този регистър съдържа цялата по- долу посочена информация:

1. името и координатите за връзка на администратора, на представителя на администратора и на длъжностното лице по защита на данните;

2. целите на обработването;

3. описание на категориите субекти на данни и на категориите лични данни;

4. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

5. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея от Регламент (ЕС) 2016/679, документация за подходящите гаранции;

6. когато е възможно, предвидените срокове за изтриване на различните категории данни;

7. когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1 от Регламент (ЕС) 2016/679.

(2) Всеки обработващ лични данни и представителят на обработващия лични данни поддържа регистър на всички категории дейности по обработването, извършени от името на администратор, в който се съдържат:

1. името и координатите за връзка на обработващия или обработващите лични данни и на всеки администратор, от чието име действа обработващият лични данни и на представителя на администратора или обработващия лични данни и на длъжностното лице по защита на данните;

2. категориите обработване, извършвано от името на всеки администратор;

3. когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея от Регламент (ЕС) 2016/679, документация за подходящите гаранции;

4. когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1 от

Регламент (ЕС) 2016/679.

Чл. 45. Регистърът се поддържа в писмена форма, включително в електронен формат.

Чл. 46. При поискване, администраторът или обработващият лични данни и представителят на администратора или на обработващия личните данни, осигуряват достъп до регистъра на надзорния орган.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. За целите на настоящите вътрешни правила „Администратор на лични данни" е ВВВУ „Г. Бенковски" представлявано от Началника.

2. Контролът по изпълнението на настоящите вътрешни правила се възлага на длъжностното лице по защита на данните.

3. Настоящите вътрешни правила се издават на основание 78 от Регламент 2016/679 и на основание чл. 25и от Закона за защита на личните данни.

4. За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните / ЕС / 2016/679, приложимото право на европейския съюз и законодателството на Република България относно защитата на личните данни.

5. Изменения и допълнения на тези правила се правят по реда на приемането им.

6. Копие от правилата са на разположение на служителите, обработващи личните данни във ВВВУ „Г. Бенковски".

7. Приложение към настоящите вътрешни правила са образци на следните документи, съставени при и по повод обработката на лични данни:

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

- Приложение № 2 Образец на заявление относно: Оттегляне на съгласие;

- Приложение № 3 Образец на заявление относно: Достъп до лични данни;

- Приложение № 4 Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите във ВВВУ правила и мерки за защита на личните данни;

- Приложение № 5 Декларация за обработка на данни от служители

на ВВВУ;

- Приложение № 6 Образец на писмо до КЗЛД относно нарушение на сигурността на личните данни;

- Приложение № 7 Образец на уведомление до администратора от страна на обработващ лични данни относно нарушение на сигурността на личните данни;

- Приложение № 8 Образец на писмо до субекта на данни за нарушение на сигурността на личните му данни.

Настоящите вътрешни правила са приети на заседание на Академичен съвет на ВВВУ „Георги Бенковски“ с протокол № 6/22.04.2020 г.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ц. сл. ЕЛЕНА ПЕНЧЕВА

____.____.2020г.

ПРИЛОЖЕНИЕ № 1 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ДЕКЛАРАЦИЯ

Долуподписаният/ата

…….....

(трите имена)

Лична карта № …….. издадена от …….…….. на ___.___.20___г.

ДЕКЛАРИРАМ:

Съгласен/а съм ВВВУ „Г. Бенковски”, гр. Долна Митрополия да обработва предоставените от мен лични данни, съгласно изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни във връзка с

……

Запознат/а съм с:

- целта и средствата на обработка на личните данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото на достъп, на коригиране и изтриване на събраните данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните;
- че района на училището е под видеонаблюдение;
- правото на подаване на жалба.

Декларирам, че давам своето съгласие за обработване на личните ми данни свободно, съгласно волята си и гарантирам верността на предоставените от мен данни и при необходимост ще оказвам съдействие на ВВВУ „Г.Бенковски” за актуализирането им.

Личните данни се съхраняват за период, не по-дълъг от необходимото за целите, за които се обработват (т. нар. принцип на „ограничение на съхранението“). След като отпадне необходимостта от използването на личните данни за целите, за които са били събрани, те се унищожават (изтриват). Съхранението им за по-дълъг срок е допустимо, когато това е предвидено в съответен нормативен акт.

Дата: ДЕКЛАРАТОР:……

гр. Долна Митрополия (подпис и фамилия)

ПРИЛОЖЕНИЕ № 2 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ДО
НАЧАЛНИКА НА ВВВУ „Г. БЕНКОВСКИ” ГР. ДОЛНА МИТРОПОЛИЯ

ЗАЯВЛЕНИЕ

относно: оттегляне на съгласие

Аз, долуподписан/ият/ата,

…….....

(*Име, презиме и фамилия*)

Лична карта № ……..….. издадена от …….…….. на ___.___.20___г.

в качеството си на „субект на лични данни“ и при условията на Общия регламент за защита на личните данни, като се има предвид, че:
Съм предоставил/а съгласието си за обработване на следните лични данни във ВВВУ „Г. Бенковски”, гр. Долна Митрополия:

…..……
……..
(посочва се точно за какви лични данни е дадено съгласие)
по следния начин:

…..……
(посочва се по какъв начин е дадено съгласието - на хартиен формуляр, по електронен път и т.н.),
във връзка със следната цел:

…..……
(изрично уточнете целите, които са декларирани при даване на съгласие за обработването на тези лични данни)
и като заявявам, че съм надлежно информиран, че имам право да оттегля съгласието си за обработване на лични данни частично или изцяло по всяко време, без да съм задължен да посочвам причина за оттеглянето.

С НАСТОЯЩОТО ВИ УВЕДОМЯВАМ, ЧЕ:

- ✓ Оттеглям съгласието си личните ми данни, посочени в това уведомление, да бъдат събирани и обработвани за посочената цел/цели.
- ✓ Декларирам, че оттеглям своето съгласие за обработване на лични данни свободно, изрично и относно всички посочени лични данни, съгласно собствената си воля и убеждение.
- ✓ Запознат/а съм, че имам право на възражения и жалби пред Комисия за защита на личните данни, която е надзорен орган в Република България, в случай, че администраторът на лични данни продължи обработването горепосочените данни след оттеглянето на съгласието с настоящото уведомление.

Дата: Заявител: ……
Гр. Долна Митрополия (подпис и фамилия)

ПРИЛОЖЕНИЕ № 3 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ДО
НАЧАЛНИКА НА ВВВУ „Г.БЕНКОВСКИ”
ГР. ДОЛНА МИТРОПОЛИЯ

ЗАЯВЛЕНИЕ

<u>относно</u>: достъп до лични данни

От .....
(Име, презиме и фамилия)
ЕГН: …..……, л. к. № ……..……..……, издадена на___.___.20___г.
от ……, адрес.....,
телефон за контакт …….., e-mail ……

МОЛЯ, на основание чл. 26 и чл. 29 от Закона за защита на лични данни, да ми бъде предоставена информация относно
…….....
…….....…,
съхранявани във ВВВУ „Г. Бенковски”, гр. Долна Митрополия
Желая да получа исканата от мен информация в следната форма:

- ⎦ преглед на информация;
- ⎦ устна справка;
- ⎦ писмена справка;
- ⎦ копия на технически носител;
- ⎦ по електронен път.

Дата: Заявител:……
гр. Долна Митрополия (подпис и фамилия)

ПРИЛОЖЕНИЕ № 4 към

Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

П Р О Т О К О Л

за преминато обучение по защита на личните данни и инструктаж за приложимите във ВВВУ „Г. Бенковски”, гр. Долна Митрополия

Вътрешни правила за мерките за защита на личните данни съгласно Регламент 2016/679

Днес,___.___.20___ г., подписаният/ата, ..., с адрес: ……., ЕГН……., на длъжност
……,

ДЕКЛАРИРАМ, ЧЕ:

1. Ми беше проведено обучение по законодателството по защита на данните и бях запознат с Вътрешните правила на ВВВУ „Г. Бенковски”, гр. Долна Митрополия “ за мерките за защита на личните данни, съгласно Регламент 2016/679.

2. Ми беше проведен инструктаж относно правилата за сигурност при обработването на лични данни и съм запознат с прилаганите от ВВВУ „Г. Бенковски”- гр. Долна Митрополия “ мерки за физическа, персонална, документална, криптографска защита на личните данни и защитата на автоматизирани информационни системи и мрежи по отношение на регистрите с лични данни, до които имам достъп при осъществяване на трудовата ми функция.

Длъжностно лице
по защита на данните: …….

Декларатор: .....

/……/

/……/

ПРИЛОЖЕНИЕ № 5 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ДЕКЛАРАЦИЯ

Долуподписаният/ата

……,
(*трите имена*)

на длъжност ……във ВВВУ „Г. Бенковски”, гр. Долна Митрополия ,

ДЕКЛАРИРАМ, ЧЕ:

1. Съм запознат/та и спазвам с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, както и прилаганата от ВВВУ „Г. Бенковски”, Политика за обработване и защита на лични данни;

2. Ще обработвам предоставените ми лични данни законосъобразно, добросъвестно и съобразно целите, за които са предоставени;

3. Няма да предоставям достъп до акаунта си и паролите си за достъп на колеги или трети лица;

4. Няма да разгласявам лични данни, до които съм получил/ла достъп при и по повод изпълнение на задълженията си;

5. Няма да ползвам за облагодетелстване на себе си или на други лица факти и обстоятелства, които съм узнал/ла при или по повод изпълнение на служебните и професионалните си задължения.

Дата: Декларатор:……

Гр. Долна Митрополия (подпис и фамилия)

ПРИЛОЖЕНИЕ № 6 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ „ГЕОРГИ БЕНКОВСКИ”
5855 гр. Долна Митрополия, обл. Плевен, телефон/факс: (064)837 217;
ул. „Св.св. Кирил и Методий” №1

Рег. № ...../ ..... 20___г.
Екз.....

ДО
ПРЕДСЕДАТЕЛЯ НА КОМИСИЯТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

УВАЖАЕМИ ГОСПОДИН ПРЕДСЕДАТЕЛ,

ВВВУ „Г. Бенковски”, ЕИК: 129011005,адрес: гр. Долна Митрополия, обл. Плевен, телефон/факс: (064)837 217; ул. „Св.св. Кирил и Методий” № 1

Длъжностно лице по защита на данните: Три имена
……

Телефон ……

E-mail…….

Адрес
……

Описание на естеството на нарушението на сигурността на личните данни:

Дата и час на узнаване на нарушението:
……..

Причина за забавяне на уведомяването (*ако има такова*)

……

Описание

……

Категории засегнати лични данни

……

Засегнати субекти (*категории и приблизителен брой*)

……

Засегнати записи на лични данни (*приблизителен брой*)

……

Последици от нарушение на сигурността на личните данни

……

Поетапно подаване на информация – ДА / НЕ

……

Предприети или предложени от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност, мерки за намаляване на евентуалните неблагоприятни последици

…….

Доказателства (описание)

……

Оценка на риска/ технически организационни мерки

……

НАЧАЛНИК НА ВВВУ „ГЕОРГИ БЕНКОВСКИ”

БРИГАДЕН ГЕНЕРАЛ ЮЛИЯН РАДОЙСКИ

___.___.20___г.

ПРИЛОЖЕНИЕ № 7 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ „ГЕОРГИ БЕНКОВСКИ”
5855 гр. Долна Митрополия, обл. Плевен, телефон/факс: (064)837 217;
ул. „Св.св. Кирил и Методий” №1

Рег. № ...../ ..... 202___г.
Екз.....

ДО
НАЧАЛНИКА НА ВВВУ„Г. БЕНКОВСКИ”
ГР. ДОЛНА МИТРОПОЛИЯ

УВЕДОМЛЕНИЕ

От ……..

обработващ лични данни

ЕИК/БУЛСТАТ/ЕГН: ..……..

Телефон ……..……..

E-mail ……..

Адрес ……..……

Уведомявам Ви, че във връзка със следната дейност по обработване на лични данни

……..

е налице нарушение на сигурността на личните данни, което се изразява в:

……..

описание на естеството на нарушението на сигурността на личните данни)

и изисква незабавно уведомяване на надзорния орган. Нарушението е установено на ……..(*дата на установяване*), и касае следните категории лични данни:

……..

Засегнати субекти (*категории и приблизителен брой*)

……..

Засегнати записи на лични данни (*приблизителен брой*)

……..

Последици от нарушение на сигурността на личните данни

……..

Предприети технически и организационни мерки във връзка с нарушението:

……..

Моля да ни уведомите какви допълнителни мерки за сигурност следва да бъдат предприети, както и каква информация и доказателства се изисква от нас.

Дата: ……
гр. Долна Митрополия (подпис и фамилия)

ПРИЛОЖЕНИЕ № 8 към
Вътрешни правила на ВВВУ за мерките за защита на личните данни съгласно Регламент 2016/679

ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ „ГЕОРГИ БЕНКОВСКИ”
5855 гр. Долна Митрополия, обл. Плевен, телефон/факс: (064)837 217;
ул. „Св.св. Кирил и Методий” №1

Рег. № ...../ ..... 20___г.
Екз.....

На вниманието на:

……..…..

(трите имена на субекта на данни)

……

(други идентификационни данни на субекта на данни)

ОТ:

Информация за Администратора:
ВВВУ „Г.Бенковски”, ЕИК: 129011005, адрес:гр. Долна Митрополия, обл. Плевен, телефон/факс: (064)837 217; ул. „Св.св. Кирил и Методий №1”
Длъжностно лице по защита на данните: Три имена
……

Телефон ……

E-mail…….

Адрес
……

Описание на естеството на нарушението на сигурността на личните данни:

……

Последици от нарушението на сигурността на личните данни:

…….

Предприети или предложени от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност, мерки за намаляване на евентуалните неблагоприятни последици

……

НАЧАЛНИК НА ВВВУ „ГЕОРГИ БЕНКОВСКИ”

БРИГАДЕН ГЕНЕРАЛ ЮЛИЯН РАДОЙСКИ

___.___.202___г.

СЪДЪРЖАНИЕ
ВЪТРЕШНИ ПРАВИЛА
ЗА СЪБИРАНЕ, ОБРАБОТВАНЕ И СЪХРАНЕНИЕ НА
ЛИЧНИ ДАННИ ВЪВ ВИСШЕ ВОЕННОВЪЗДУШНО УЧИЛИЩЕ „ГЕОРГИ БЕНКОВСКИ ”