УТВЪРДИЛ:
РЕКТОР
ПРОФ. НИКОЛАЙ ИЗОВ, ДОКТОР

ПРОЦЕДУРА ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИ В НАЦИОНАЛНА СПОРТНА АКАДЕМИЯ „ВАСИЛ ЛЕВСКИ“

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Всички дейности, които включват обработване на лични данни, или всички действия, които засягат обработването на лични данни и оказват въздействие върху неприкосновеността на личния живот на субектите на данните, попадат в обхвата на настоящата процедура и ще бъдат обект на оценка на въздействието върху защитата на данните, съгласно изискванията на тази процедура.

Чл. 2. (1) Оценка на въздействието е необходимо да се извърши при всяко въвеждане или смяна на ключова система или програма, която е свързана с обработката на лични данни, включително:
а) първоначално въвеждане на нови технологии или прехода към нови технологии;
б) автоматично обработване, включително профилиране или автоматизиране на решенията;
в) мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;
г) системно мащабно наблюдение на публична обществена зона.
(2) Оценката на въздействието задължително се извършва и при обработване на лични данни от системите за видеонаблюдение.

II. ЗАДЪЛЖЕНИЯ

Чл. 3. (1) Всяко лице, което обработва лични данни от името на Администратора, трябва да уведоми незабавно длъжностното лице по защита на личните данни, когато подозира или установи рискове за сигурността на личните данни.
(2) Администраторът носи отговорност за извършването на оценка на въздействието върху защитата на данните.
(3) При извършването на оценка на въздействието Администраторът задължително изисква становище на длъжностното лице по защита на данните по следните въпроси:
- дали да извърши оценка на въздействието върху защитата на данни или не;
- каква методика да използва при извършването на оценка на въздействието върху защитата на данни;
- дали да извърши оценка на въздействието върху защитата на данни вътрешно, или да я възложи на външен изпълнител;

• какви гаранции (включително технически и организационни мерки) да приложи, за да намали до минимум всички рискове за правата и интересите на субектите на данните;
• дали оценката на въздействието върху защитата на данните е направена правилно и дали заключенията от нея (дали да се продължи с обработването и какви гаранции да се приложат) показват спазване на Общия регламент за защита на личните данни;
(4) Длъжностното лице по защита на лични данни при поискване предоставя съвети по отношение на извършването на оценка на въздействието върху защитата на данните, както и наблюдава самото ѝ извършване.
(5) Ръководителят на съответната дейност по обработка на данните в организацията и/или длъжностното лице по защита на личните данни могат с писмен доклад да предложат на Администратора да извърши оценка на въздействието върху защитата на данните по отношение на конкретна операция по обработване, да подпомогнат оценяването на качеството на оценката на риска, както и да предоставят данни за оценката.
(6) Оценката на въздействие се извършва от длъжностното лице по защита на личните данни или от външен доставчик на услуги и се обективира в доклад.
(7) При особени обстоятелства, когато съществува висок риск при обработването да бъдат засегнати права и интереси на субектите на данни, Ректорът определя комисия от лица с различна професионална квалификация.
(8) Минималният състав на комисията включва длъжностното лице по личните данни, юрист, специалист по информационна сигурност или системния администратор, лице на ръководна позиция.
(9) В заповедта по ал. 7 се определя ръководител на дейността на комисията и той координира цялата процедура по извършването на оценка на въздействието върху защитата на данните.
(10) В случай, че обработването на лични данни се извършва изцяло или частично от обработващ лични данни, обработващият лични данни подпомага администратора при извършването на оценката на въздействието и предоставя цялата необходима информация.

II. АНАЛИЗ НА РИСКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЕ

Чл. 4. (1) Анализът на риска осигурява информацията, необходима за вземането на решения относно избора на най-подходящите мерки и методи на въздействие спрямо определения риск. Процесът се състои в определяне на последствията и вероятността за възникване.
(2) Администраторът извършва оценка на въздействието на лични данни с цел определяне на адекватно ниво на технически и организационни мерки за защита на личните данни, което отговаря на обработваните от него лични данни и въздействието при нарушаване на защитата им.
Чл. 5. (1) Оценката на въздействието е процес, при който се извършва преценка на нивата на рисковете за правата и свободите на субектите на данни. Водещ критерий при тази преценка е нивото на въздействие, което нарушаването на поверителността, цялостността или наличността на личните данни би оказало върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица.

(2) При извършването на оценката на въздействието се използва следната методология за степенуване на въздействието (риска), отчитаща вероятността за настъпване на съответното нарушение на сигурността на данните (вероятност) и потенциалните неблагоприятни последици (въздействие):
(3) В зависимост от определеното ниво на въздействие се извършва:
1. приоритизация на идентифицираните рискове, и
2. определя адекватно ниво на защита, включващо техническите и организационните мерки, които трябва да предприеме за тяхното ограничаване.
(4) Длъжностното лице по защита на личните данни анализира вероятността за възникване на нарушение на сигурността на данните и определя 4 (четири) нива на въздействие – ниско, средно, високо и изключително високо.
Чл. 6. Редът на приоритет на идентифицираните рискове е, както следва:
т. 1. Рисковете с висока тежест на последиците и вероятност за настъпване (8, 9, 11 и 12) трябва да бъдат напълно избегнати или ограничени чрез прилагане на мерки за сигурност, които намаляват както тежестта им, така и тяхната вероятност. В плана за действие на рисковете се предвиждат както мерки за предотвратяване (действия, предприети преди вредно събитие), така и за защита (действия, предприети по време на вредно събитие) и възстановяване (действия, предприети след вредно събитие).
т. 2. Рисковете с висока тежест, но с малка вероятност (6, 10) трябва да се избягват или ограничават чрез прилагане на мерки за сигурност, които намаляват тежестта на последиците или вероятността за настъпването им. Приоритет следва да имат преди всичко мерките за предотвратяване (превантивните мерки).
т. 3. Рисковете с малка тежест, но с голяма вероятност за настъпване (3, 7) трябва да бъдат ограничавани чрез прилагане на мерки за сигурност, които намаляват тяхната вероятност. Трябва да се наблегне обаче на мерките за възстановяване.
т. 4. Рискове с ниска тежест и вероятност (1, 2, 4, 5) могат да бъдат третирани на по-късен етап, още повече че прилагането на мерките спрямо рисковете с по-висок приоритет може да доведе до тяхното елиминиране или значително ограничаване.
Преценяването на риска се прави с цел да се определят значимостта и видът на риска и да се вземат решения за бъдещи действия.
Чл. 7. Нивата на въздействие са, както следва:
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. 8. (1) На база оценката на нивото на въздействие се определя съответното ниво на защита, което представлява съвкупност от технически и организационни мерки за защита на личните данни.
(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.
(3) След определяне на съответното ниво на защита е необходимо да се въведе минималното ниво на технически и организационни мерки, отговарящи на определеното ниво и съответстващи на изискванията на нормативната уредба по отношение на видовете защита на личните данни.
(4) Оценка на риска се извършва на основата на:
• естеството, обхвата, контекста и целите на обработването;
• възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест;
• последиците за правата и свободите на физическите лица.
Чл. 9. (1) Въз основа на оценката на риска длъжностното лице по защита на данните предлага на Ректора план за действие за въвеждане на определените технически и организационни мерки, които да бъдат ефективни и способни за реализиране в рамките на предприятието.
(2) Планът за действие за въвеждане на определените технически и организационни мерки включва:
• определянето на мерки за елиминирането или ограничаването на съществуващите рискове, както и на тези, които могат да възникнат в бъдеще;
• определяне на отговорник и екип;
• определяне на срокове за изпълнение на мерките и етапи за изпълнение.
(3) Освен при започване на нова дейност, оценка на въздействието се прави и при всяка промяна в риска, с който са свързани вече съществуващи операции по обработване.

III. СЪДЪРЖАНИЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕ

Чл. 10. Оценката на въздействие върху данните съдържа най-малко следното:
• системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
• оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
• оценка на рисковете за правата и свободите на субектите на данни; и
• мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на Общия регламент за защита на данните.

Чл. 11. При извършването на оценка на въздействието върху защитата на данните се вземат предвид следните критерии, предложени от Работната група по чл. 29 по прилагането на Общия регламент, така че същата да отговаря на изискванията на Общия регламент за защита на данните:

т. 1. системен опис на обработването (член 35, параграф 7, буква а) на Общия регламент включва:

• вземат се предвид естеството, обхватът, контекстът и целите на обработването;
• поддържа ли се регистър на личните данни, получателите и срока, за който ще се съхраняват личните данни;
• осигурено е описание на операцията по обработване;
• определени са елементите, свързани с личните данни;
• взема се предвид спазването на одобрени кодекси за поведение, ако е приложимо;

т. 2. оценка на необходимостта и пропорционалността (член 35, параграф 7, буква б) на Общия регламент включва:

• определени са мерки за спазване на принципите на Общия регламент;
• определени са мерки, допринасящи за правата на субектите на данни;

т. 3. оценка на рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква в) включва:

• оценяват се произходът, естеството, спецификата и степента на рисковете от гледна точка на субектите на данни:
• определя се източникът на риска;
• потенциалните въздействия върху правата и свободите на субектите на данни, в случай на определени събития, включително незаконен достъп, нежелани изменения и изчезване на данни;
• изчисляват се вероятността и тежестта;
• определят се мерки за третиране на рисковете.

V. ПРЕДВАРИТЕЛНА КОНСУЛТАЦИЯ

Чл. 12. Когато в резултат на извършена оценка на въздействието, преди започването на обработката на лични данни, се установи, че обработката им ще доведе до висок риск за субектите на данни, ако не бъдат предприети адекватни мерки за ограничаване на риска, администраторът, чрез длъжностното лице по защита на данните, се консултира с надзорния орган, съгласно изискванията на чл. 36 от Общия регламент.

Чл. 13. При консултация с надзорния орган се предоставя следната информация:

• информация за отговорностите на организацията и лицата, които се занимават с обработването;
• целите на планираното обработване;
• информация за всякакви/всички мерки и контроли, които се прилагат/ предоставят за защита на правата и свободите на субектите на данни;
• копие от оценката на въздействието върху защитата на данните и всякаква друга информация, поискана от надзорния орган.

VI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Процедурата за оценка на въздействието върху защитата на данните е приета с Решение по Протокол № 41/02.12.2021г. от Ректорски съвет.

§ 2. Настоящата процедура се изменя своевременно при изменение на нормативната уредба, свързана със защита на личните данни.

§ 3. За неуредените в тази процедура въпроси се прилагат разпоредбите на действащата нормативна уредба.