

УТВЪРДИЛ:
ИАНА СТОЯНОВА
ДИРЕКТОР НА НТБГ

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В НАЦИОНАЛНА ТЪРГОВСКО-БАНКОВА ГИМНАЗИЯ (НТБГ)

В съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните – GDPR)

Чл. 1. Основни цели и принципи

(1) Настоящите Вътрешни правила са разработени в съответствие със стремежа на Националната търговско-банкова гимназия (НТБГ) да прилага високи стандарти за защита на личните данни на национално и европейско ниво като неразделна част от своята институционална политика спрямо ученици, родители, служители, преподаватели и партньори.

(2) С оглед характера на дейността си НТБГ действа като администратор и/или обработващ лични данни, поради което гарантира, че всички процеси по обработване на лични данни са:

- законосъобразни;
- прозрачни;
- сигурни;
- ограничени до конкретни и легитимни цели.

(3) Настоящите правила отразяват принципите по чл. 5 от GDPR и приложимото национално законодателство, включително Закона за защита на личните данни.

(4) Всички служители на НТБГ са длъжни да спазват тези правила при изпълнение на служебните си задължения.

Чл. 2. Лице, отговорно за защитата на личните данни

(1) НТБГ определя лице, отговорно за защитата на личните данни, което:

- следи за прилагането на техническите и организационните мерки за защита;
- съдейства при упражняване на правата на субектите на данни;
- координира действията при инциденти с лични данни.

(2) Лицето по ал. 1 се определя със заповед на директора на НТБГ.

(3) Длъжностно лице по защита на данните по смисъла на чл. 37 от GDPR е: Нейчо Ангелов Попов – заместник-директор по АСД на НТБГ.

Основни категории субекти и видове лични данни

Чл. 3. Лични данни на ученици и родители

(1) НТБГ събира и обработва лични данни на:

- кандидати за ученици;
- ученици;
- родители/настойници/попечители,

с цел администриране на приема, обучението и свързаните с него дейности, съгласно нормативната уредба на МОН.

(2) На учениците и родителите се предоставя информация по чл. 13 и 14 от GDPR относно:

- вида на събираните данни;
- целите на обработването;
- правата на субектите на данни.

(3) Информацията се предоставя чрез:

- информационно табло в НТБГ;
- интернет страницата на гимназията;
- брошури, предоставяни от класните ръководители;
- заявления за участие в събития и инициативи.

(4) Личните данни се предоставят на трети лица само при наличие на законово основание или легитимен интерес и при спазване на изискванията на GDPR.

Чл. 4. Лични данни на партньори и контрагенти

(1) НТБГ събира и обработва лични данни на:

- партньори – физически лица;
- законни представители и пълномощници на партньори – юридически лица,

на основание изпълнение на договор или преддоговорни отношения.

(2) Данните се събират при сключване на договор или при подготовка за такъв.

(3) Данните на законните представители могат да бъдат получавани и от публични регистри (Търговски регистър, регистри на държавни органи).

(4) Обработват се само минимално необходими данни – имена, длъжност, служебни координати.

(5) Документите се съхраняват в помещения и информационни системи с контролиран достъп.

Чл. 5. Лични данни на служители и лица по граждански договори

(1) НТБГ обработва лични данни на служители и лица по граждански договори на основание изпълнение на договор и законови задължения.

(2) На служителите се предоставя задължителната информация по чл. 13 от GDPR.

(3) Не се събират копия от лични карти. В случай че такива са били събрани в минал период, същите се унищожават.

(4) Данните се съхраняват в трудови досиета при спазване на законово определените срокове.

(5) Данни за здравословно състояние се обработват само при наличие на законово основание и при засилени мерки за защита.

Чл. 6. Лични данни на кандидати за работа

(1) Данните на кандидати за работа се обработват за целите на подбор и назначаване.

(2) Кандидатури на неodobрени кандидати се унищожават след приключване на подбора, освен ако не е дадено изрично съгласие за по-дълго съхранение.

(3) Данните не се използват за други цели и не се включват в маркетингови бази.

Чл. 7. Лични данни, обработвани от счетоводството

(1) Счетоводството обработва лични данни само в обем, необходим за:

- изплащане на възнаграждения;
- осигуряване;
- счетоводна отчетност.

(2) Достъп имат само оправомощени лица.

(3) Данните се съхраняват при засилени технически и организационни мерки.

Чл. 8. Лични данни, обработвани от ИТ звеното

(1) ИТ персоналът няма право на съдържателен достъп до лични данни.

(2) Достъпът е ограничен до поддръжка и администриране на системи.

Чл. 9. Канцелария

(1) Лични данни на податели и получатели се обработват на основание легитимен интерес.

(2) Срокът на съхранение е до 1 година, освен ако закон не предвижда друго.

Чл. 10. Учебен процес и прием

(1) НТБГ обработва лични данни във връзка с приема, обучението и оценяването на учениците.

(2) Данните се съхраняват:

- до завършване на обучението – за приетите ученици;
- до 1 година – за неприетите кандидати.

(3) Забранява се публичното оповестяване на списъци с лични данни.

Чл. 11. Библиотека

(1) Библиотеката обработва лични данни за обслужване на ученици и учители.

(2) Данните се съхраняват при контролирани условия и не се предоставят на трети лица.

Чл. 12. Събиране и съхранение на лични данни

(1) Данните се събират на законово основание по чл. 6 от GDPR.

(2) Съхраняват се само за срока, необходим за постигане на целите.

Чл. 13. Обработване и оценка на риска

(1) Данните се обработват само за първоначално заявените цели.

(2) При необходимост се извършва оценка на въздействието.

Чл. 14. Права на субектите на данни

Субектите имат всички права по глава III от GDPR, включително:

- достъп;
- коригиране;
- изтриване;
- ограничаване;
- възражение;
- преносимост.

Чл. 15. Упражняване на права

(1) Исканията се подават писмено.

(2) Самоличността се удостоверява без копиране на документи.

(3) Отговор се предоставя в законовите срокове.

Чл. 16. Достъп на служителите

(1) Всеки служител има индивидуален служебен достъп.

(2) Достъпът се ограничава според длъжността.

Чл. 17. Обучение и инструктаж

(1) Провеждат се регулярни обучения по защита на личните данни.

Чл. 18. Технически и организационни мерки

(1) Прилагат се мерки по чл. 32 от GDPR.

(2) Извършва се архивиране и контрол на достъпа.

Чл. 19. Нарушения на сигурността

(1) Нарушенията се докладват незабавно.

(2) КЗЛД и субектите се уведомяват при необходимост.

Чл. 20. Заключителни разпоредби

Настоящите правила влизат в сила от датата на утвърждаването им със заповед на директора.