ПОЛИТИКА ЗА НЕПРИКОСНОВЕНОСТ И ЗАЩИТА НА ДАННИТЕ НА БЪЛГАРСКА НАЦИОНАЛНА АСОЦИАЦИЯ „ЕТЕРИЧНИ МАСЛА, ПАРФЮМЕРИЯ И КОЗМЕТИКА“

УВОД

В ежедневната си дейност Българската Национална Асоциация „Етерични Масла, Парфюмерия и Козметика“ (БНАЕМПК) използва различни данни, чрез които могат да бъдат идентифицирани лица, включително:

- настоящи, минали и бъдещи работници/служители;
- служители на фирми членове на БНАЕМПК;
- членове на Управителния и Контролния съвет;
- лица от списъка с експерти на БНАЕМПК;
- трети засегнати лица.

Поради събирането и използването на тази информация, организацията е адресат на многобройни законови разпоредби, които уреждат методите за извършване на дейностите по обработка на данните и предпазните мерки, които следва да бъдат осигурени.

Целта на тази политика е да бъде определено релевантното законодателство и да опише действията, които БНАЕМПК трябва да предприеме, за да постигне съответствие с изискванията.

Контролът, съгласно настоящата политика, се разпростира върху всички звена, лица и процеси в рамките на информационните системи на организацията, включително управителни органи, директори и ръководни органи, персонал, доставчици и други трети страни, които имат достъп до системите на организацията.

1. Общ регламент за защита на данните (GDPR)

Общият регламент за защита на данните (GDPR) е един от най-значимите законодателни актове, уреждащи дейността по обработване на данни. Регламентът предвижда санкции в големи размери в случай на пробив в сигурността на данните (в случай, че организацията не е положила дължимата грижа). Чрез настоящата политика БНАЕМПК се стреми да осигури, поддържа и демонстрира съответствие с изискванията на GDPR и относимото законодателство по всяко време.

2. Легални дефиниции

В GDPR се съдържат общо 26 легални дефиниции и не е практично всички те да бъдат поместени в настоящата политика. По-ключовите понятия обаче биха намерили място и затова са представени по-долу:

"Личните 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;

"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;

"Администратор на лични данни"

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.

"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.

3. Основни принципи при обработването на лични данни

Следните принципи са широко застъпени в GDPR:

1. Личните данни трябва да бъдат:

♦ обработвани законосъобразно, добросъвестно и прозрачно по отношение на субекта на данни *("законосъобразност, добросъвестност и прозрачност");*

♦ събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели *("ограничение на целите");*

♦ подходящи, свързани със и ограничени до необходимото във връзка с

целите, за които се обработват *("свеждане на данните до минимум");*

♦ 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");*

♦ 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, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните *("ограничение на съхранението");*

♦ 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");*

2. Администраторът носи отговорност и е в състояние да докаже спазването на принципите *("отчетност").*

БНАЕМПК гарантира, че зачита и спазва принципите, както при използването на настоящите методи за обработка на данни, така и при разработването на нови такива (напр. нови софтуерни решения).

4. Права на субекта на данни

GDPR предоставя определени права на субектите на данни. Обобщено те са:

♦ право да бъдат информирани;

♦ право на достъп;

♦ право на коригиране на съществуващите данни;

♦ право на изтриване на данните ("правото да бъдеш забравен");

♦ право за ограничаване на обработването на данните;

♦ право на преносимост на данните;

♦ право на възражение;

♦ права във връзка с автоматизираното обработване на данни и профилирането.

Упражняването на всяко от описаните права е свързано с процедура на БНАЕМПК, която позволява необходимите действия да бъдат предприети във времевите рамки, установени от GDPR (таблица 1).

Таблица 1 - Права на субектите на данни	
Искане от субекта на данни	**Времева рамка**
Право да бъде информиран	Веднага, ако данните са предоставени директно от субекта, или в рамките на един месец, ако са предоставени от друго лице
Право на достъп	Един месец
Право на коригиране на съществуващите данни	Един месец
Право на изтриване на данните ("правото да бъдеш забравен")	Във възможно най-кратки срокове след постъпване на искането
Право за ограничаване на обработването на данните	Във възможно най-кратки срокове след постъпване на искането
Право на преносимост на данните	Един месец
Право на възражение	Веднага след постъпване на възражението
Права във връзка с автоматизираното обработване на данни и профилирането	Варира в зависимост от същността на искането

5. Законосъобразност на обработването

GDPR съдържа шест алтернативни основания, които правят обработката законосъобразна, в зависимост от конкретните обстоятелства. БНАЕМПК обработва данни само на посочените основания в зависимост от случая, като документира връзката между основанието и обстоятелствата в съответствие с GDPR. Алтернативите са описани накратко по-долу.

5.1. Съгласие

Ако е необходимо за цели, признати от GDPR, БНАЕМПК ще се стреми да получава изрично съгласие от субектите на данни, за да събира и обработва техни данни. В случай, че се отнася до данни на деца, необходимо е съгласие и от родител/настойник. Пълна информация относно политиката по обработка на данни и относно използването на техните данни ще бъде предоставена на субектите в момента на получаване на тяхното съгласие. Допълнително ще им бъдат обяснени

правата, които получават във връзка с даденото съгласие, като например правото да го оттеглят по всяко време. Посочената информация следва да бъде предоставяна в подходяща форма, да бъде описана на разбираем език и да бъде безплатна.

Ако данните не бъдат получени директно от субекта, за когото се отнасят, тази информация следва да му бъде съобщена в разумен период от време, но не по-късно от един месец от получаване на данните.

5.2. Изпълнение на договор

Когато събраните и обработвани данни са необходими за изпълнението на договор със субекта на данни, изрично съгласие не е нужно. Това основание е приложимо в случаите, когато предоставените данни са жизнено важни за изпълнението на договора (напр. доставката не може да бъде направена без адрес на лицето).

5.3. Законово задължение

Когато личните данни са събирани и обработвани, за да бъде изпълнено законово задължение, изрично съгласие не е необходимо. Това основание е приложимо в областта на трудовото, данъчното и, като цяло, публичното право.

5.4. Жизненоважни интереси на субекта на данни

Законосъобразно е да получим и обработим лични данни, ако те са необходими за защита на жизненоважни интереси на субекта на данни или на друго физическо лице. БНАЕМПК ще обработва лични данни на това основание само в случай, че наистина са засегнати жизненоважни интереси, като обстоятелствата ще бъдат детайлно документирани, така че да бъде доказуемо.

5.5. Изпълнение на задача от обществен интерес

Когато БНАЕМПК трябва да изпълни задача, която вярва, че е в обществен интерес, или е част от служебно задължение, съгласие от субекта на данни няма да бъде поискано. Преценката дали се касае за обществен интерес и/или служебно задължение, се документира и може да служи като доказателство при нужда.

5.6. Легитимен интерес

БНАЕМПК може да обработва данни за защита на легитимен интерес, в случай, че не се засягат в значителна степен правата и свободите на субектите на данни. И в този случай преценката дали един интерес е легитимен и относно степента на засягане на правата и свободите на субектите на данни следва да бъде документирана.

6. Защита на етапа на проектиране

БНАЕМПК зачита принципа за защита на етапа на проектиране. Планирането

и изграждането на всички нови или на съществено променени съществуващи системи, които събират, съхраняват или обработват данни, ще бъде оценявано от гледна точка на евентуални проблеми за сигурността. За всеки проект ще бъде правена оценка на въздействието върху защитата на данни и ще бъдат взети подходящите мерки за защита срещу нарушения.

Оценката на въздействието върху защитата на данни включва:

● Преглед на методите за обработка на личните данни и целите;

● Преценка дали очаквания метод за обработка на данни е приложим и подходящ за посочената цел;

● Оценка на риска за субектите на данни при обработване на данните им;

● Какъв контрол и какви мерки за сигурност са необходими, за да се минимизира идентифицирания риск и да се постигне съответствие с изискванията на GDPR.

Добрата практика е, при възможност, да бъдат използвани техники като псевдонимизиране и съхраняване само на необходимата информация.

7. Договори, включващи обработка на лични данни

БНАЕМПК ще гарантира, че всички договори, които сключва и в чиито обхват попада обработка на лични данни, ще съдържат необходимата информация и общи условия, изискуеми от GDPR.

8. Международен трансфер на данни

Трансферът на данни извън Европейския съюз ще бъде внимателно обмислян преди фактическото му осъществяване, за да се гарантира, че попада в границите, поставени от GDPR. Всеки конкретен случай се разглежда отделно, тъй като зависи от преценката на Европейската комисия към момента за нивото на сигурност, което третата държава предоставя по отношение на личните данни.

9. Длъжностно лице по защита на данните

GDPR задължава всяка организация, която е публична, която обработва голям обем лични данни или събира/съхранява "чувствителни" данни да има длъжностно лице по защита на данните. Последното следва да има необходимия обем знания и умения за целите на GDPR, но може да бъде както лице от самата организация, така и външно лице. Съобразно поставените от регламента изисквания, БНАЕМПК не трябва да ангажира длъжностно лице по защита на данните.

10. Уведомление за нарушение на сигурността на данните

В случай на пробив в сигурността на данните, БНАЕМПК предприема необходимите действия, за да предупреди засегнатите лица. Действията следва да бъдат пропорционални на нарушението, като следва да се спазва и принципът за

прозрачност. GDPR задължава организацията, в случай на пробив, който може да застраши правата и свободите на лицата, да уведоми надзорния орган (Комисията за защита на личните данни) в рамките на 72 часа от узнаването. Уведомяването се извършва в съответствие с нарочна процедура, разписана от БНАЕМПК. Санкциите за нарушение на разпоредби на регламента достигат до четири процента от общия годишен оборот или до двадесет милиона евро (която от двете суми е по-висока).

11. Постигане на съответствие с GDPR

Следните действия са предприети от БНАЕМПК, за да бъде постигнато пълно съответствие с изискванията на GDPR:

- Анализирано е законодателството в областта на личните данни
- Работниците/служителите, които се занимават с обработване на лични данни, разбират задълженията си и отговорността за спазването на политиките и процедурите за защита на личните данни на организацията
- Персоналът е инструктиран относно необходимото ниво на защита на данните
- Спазват се правилата за съгласие на субектите на данни
- Предоставени са възможности за упражняване на правата от субектите на данни и техните искания се управляват ефективно
- Извършват се периодични прегледи с цел актуализация на политиките/процедурите относно защитата на личните данни
- Спазва се принципът за защита на етапа на проектирането за всички нови или драстично променени системи и процеси
- Води се следната документация за дейностите по обработване:
  - Името на организацията и други необходими детайли
  - Цели на обработването на данни
  - Категории лица и обработвани техни лични данни
  - Категории обработващи лични данни
  - Споразумения и механизми за трансфер на данни към страна извън Европейския съюз
  - Срокове за съхранение на лични данни
  - Организационни и технически мерки за осигуряване на защита на данните.

Посочените дейности следва периодично да се преглеждат като част от общия одит на защитата на данните, извършват от ръководните органи.