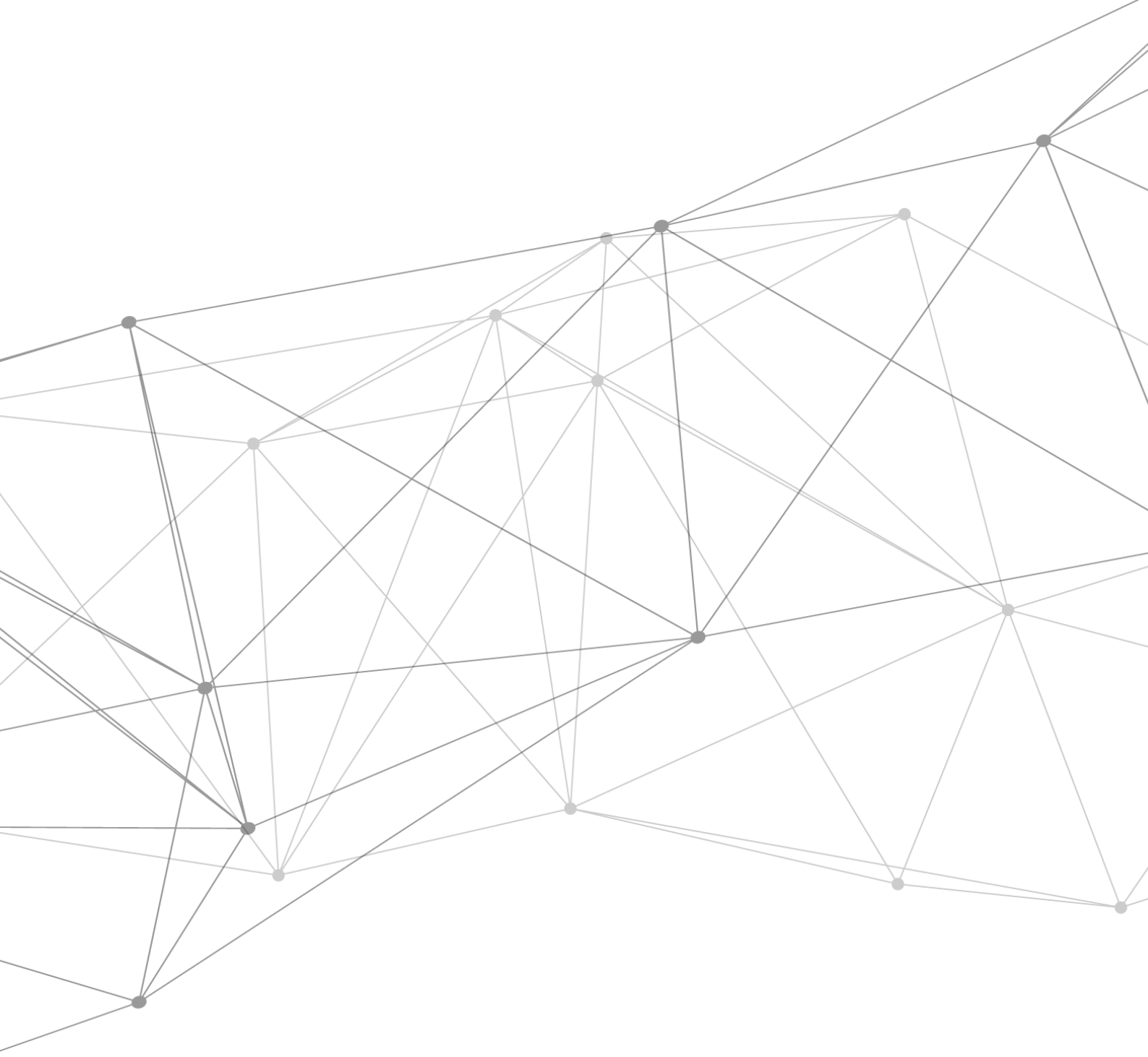

GDPR СЕКТОРЕН КОДЕКС

iab bulgaria

СЕКТОРЕН КОДЕКС ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДИГИТАЛНИЯ СЕКТОР

РАЗРАБОТЕН ОТ ИНТЕРАКТИВ БЮРО БЪЛГАРИЯ

ЗА ОДОБРЕНИЕ ОТ КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В БЪЛГАРИЯ

Съдържание

Преамбюл

Interactive Advertising Bureau Bulgaria (ИАБ) обединява основните участници от дигиталния сектор, като в практиката си е установило високи професионални и етични стандарти и насоки, които да се спазват от неговите членове и участниците на дигиталния пазар в България. Основна цел на ИАБ България е да осигури хармонизация между законодателната рамка и бизнеса, като си сътрудничи с частни и публични субекти, включително държавни органи.

Участниците на пазара на уеб и дигитални услуги в България предоставят широк спектър от услуги, като в хода на дейността им се събират и обработват разнообразни видове и обем от данни, които са необходими за оптималното предоставяне на съответните услуги. Обработването на лични данни и досега е следвало стриктни принципи и стандарти, гарантиращи спазването на законовите изисквания и правата и интересите на субектите на данни. С началото на прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (GDPR), се въвеждат допълнителни изисквания, които дигиталният бизнес трябва да изпълни, за да осигури регулаторно съответствие на дейността си.

Спецификите на дигиталния сектор, техническите характеристики, разнообразието на връзки и взаимосвързаност между дружествата, с цел осигуряване на пълна функционалност на предоставяните услуги на потребителите, налагат синхронизирането на привеждането в съответствие с GDPR на специфичната дейност на участниците на дигиталния и онлайн пазар. Именно това е целта на този Секторен кодекс, чието приложение и спазване ще гарантира съответствие с GDPR, защита на правата и интересите на субектите на лични данни, интегриране на единни високи стандарти за обработка на личните данни, прозрачност на бизнес процесите и сигурност при предоставянето на услуги на информационното общество и по-конкретно в дигиталния сектор. Чрез Секторния кодекс ще се постигне баланс между правата и интересите на физическите лица – потребители на услуги от една страна и икономическите потребности и растеж на бизнеса.

Водени от горното и в съответствие с предвидената в GDPR възможност за саморегулиране при изпълнение на изискванията за защита на личните данни ИАБ България и Комисията за защита на личните данни в България одобриха този кодекс.

Раздел I

Съгласие за обработка на лични данни

Чл. 1. (1) Администраторът осигурява възможност на субекта на данните да предостави по електронен път съгласието си за обработка на личните данни чрез регистрационна форма, която осигурява механизми за изрично изразяване на съгласието с всяка една отделна цел на обработка на данните.

(2) Формата за предоставяне на съгласие осигурява достъп до информация относно правата на субекта на данните във връзка с обработката на личните му данни (Privacy notice). Тази информация се предоставя чрез поставяне на видимо място на линк към страница в Интернет или попъп (pop-up) в регистрационната форма на Администратора. Счита се, че Администраторът е изпълнил изискванията за предоставяне на информация за правата на субекта на данните, ако е осигурил линк или попъп във формата за регистрация за получаване на съгласие за обработка на данните.

(3) Субектът на данните изразява съгласието си за събиране и обработване на данните му за конкретно посочените цели изрично чрез натискане на бутон или чекбокс (check box) в регистрационната форма на Администратора. Бутоните, чекбоксовете или другите елементи в регистрационната форма не може да са конфигурирани да изразяват съгласие по подразбиране от субекта на данните без неговата изрична реакция или изявление. Това не ограничава Администратора да осигурява функционалност на сайта за улеснено изразяване на съгласие за отделните видове обработка, като например бутон за избиране едновременно на всички цели на обработка, маркиране на множество цели с едно натискане на бутон или други сходни функционалности.

(4) Формата за изразяване на съгласие и елементите на интерфейса или дизайна й, могат да са на език, различен от български, ако субектът на данните е заявил разбирането си на този език или от обстоятелствата може да се съди, че субектът на данните разбира този език.

(5) Съгласието за обработка на личните данни или посочване на цели за обработка може да бъде поискано от Администратора във всяка една фаза от процедурите за регистрация в сайт, за използване на услуга или сключване на договор чрез електронни средства, но преди или най-късно към момента на завършване на регистрацията или сключването на договора.

Чл. 2. (1) В случай на събиране на лични данни от субект, който декларира, че е под 16 навършени години, Администраторът осигурява допълнителен механизъм за потвърждение на съгласието на обработка на личните данни от родител или настойник на детето чрез имейл за получаване на съгласие от родителя на детето. За тази цел администраторът информира детето – субект на лични данни, че за да бъде завършена регистрацията и да бъде предоставена услугата, е необходимо съгласие на неговия родител или настойник, чийто имейл адрес или телефон за връзка субектът трябва да предостави. В този случай Администраторът може да използва и услуги на трети лица за получаване на съгласие от родител. Администраторът изпраща напомнително уведомление до родителя/настойника и субекта на данните преди датата на навършване на 16 години от детето, когато изтича срока на съгласието, с оглед получаване на ново съгласие от субекта на данните (детето).

(2) Освен ако няма обосновани съмнения в родителските права на лицето, посочено от субекта на данните, Администраторът приема съгласието и завършва регистрацията или предоставя услугата. В случай на обосновани съмнения, Администраторът може да поиска допълнителна информация.

Чл. 3. (1) За целите на изпълнението на задълженията си по този кодекс, Администраторът може да прилага примерните форми за изразяване на съгласие, представляващи Приложение № 1 към този кодекс.

(2) Администраторът може да използва автоматични средства за получаване на съгласие от субекта на данните, като например браузър, системи за предоставяне на съгласие за обработка на лични данни и идентификация в социални мрежи (например facebook, linked-in и други), услуги за управление на личните данни или приложения, както и Централизираната единна система за предоставяне на съгласие, разработена от IAB Европа.

(3) Администраторът може да изисква общо съгласие от субекта на данните за обработката им чрез обработващ лични данни. Съгласието се получава от Администратора чрез изрично изявление за съгласие или чрез клауза в договора за използване на услугата или получаване на информацията от администратора. В този случай, Администраторът поддържа на сайта си актуален списък на лицата, на които възлага обработването на личните данни с уникални идентификатори, данни за контакт и посочване какви лични данни им се предоставят за обработка, като не е необходимо допълнително уведомяване на субекта, включително при актуализиране на списъка, доколкото информацията е по всяко време достъпна.

Чл. 4. (1) Администраторът запазва съгласието на субекта на данните за обработка на личните данни в електронна форма.

(2) Счита се, че Администраторът е доказал безспорно получаването на съгласие за обработка на личните данни, ако субектът на данните е потвърдил съгласието си по имейл, включително ако е натиснал линк в имейл, изпратен му от Администратора, с което изрично е заявил воля за съгласие за обработка на личните му данни за определените в имейла цели и категории данни. Записването на съгласието може да се извършва от Администратора в база данни за съгласия на субектите на данните чрез запис на идентификатор, час на предоставяне на съгласие и лице, за което се отнасят.

(3) Заедно с или вместо горните способи, Администраторът може да използва други методи за доказване на получаването на съгласие, като например: SMS верификация, електронен подпис, карта за електронна идентичност, биометрични идентификатори на мобилни устройства, визуално сканиране, устно съгласие чрез звукозапис или видеозапис и други сходни технологии.

Раздел II

Събиране на лични данни

Чл. 5. (1) Администраторът осигурява, доколкото е технически или правно възможно и допустимо, че услугите, които предоставя на субекта на данните, могат да се използват и без събиране на лични данни, ако субектът на данните изрази изричното си изявление за това или откаже да предостави лични данни.

(2) За целите на изпълнение на ал. 1, Администраторът осигурява възможност на субекта на данните да не предоставя всички изискуеми лични данни във формата за предоставяне на съгласие за обработката им, като отбелязва по подходящ начин задължителната и незадължителната информация, която субектът трябва или може да предостави.

(3) Администраторът има право да откаже предоставянето на услугата или достъпа до сайт без регистрация или предоставено съгласие за обработка на лични данни от субекта на данните, включително, но не само в следните случаи:

- Необходима е индивидуализация на субекта на данните за целите на получаване на плащания от него и издаване на счетоводни документи;
- Предоставяната услуга изисква индивидуализация на субекта на данните, за целите на нормалното и качествено функциониране на услугата;
- Необходима е индивидуализация на субекта на данните за целите на изпълнение на изискванията за предоставяне на информация или упражняване на правата на субекта на данните по GDPR или приложимото право;
- Исканата информация е необходима за изпълнение на задължения на Администратора, които той има съгласно приложимото законодателство.

(4) Администраторът събира от субектите на данните само такива лични данни, които са му необходими за предоставяне на услугата или изпълнение на договора със субекта на данните. Ако Администраторът събира повече данни от тези, които са му необходими за предоставяне на услугата или изпълнението на договора, субектът на данните трябва да изрази своето изрично съгласие по електронен път, а Администраторът осигурява, че предоставянето на услугата или изпълнението на договора ще бъде осигурено и без събирането на тези данни и без да е дадено съгласие за тяхната обработка или при оттеглено такова съгласие.

Чл. 6. (1) В случай че Администраторът не събира лични данни за цели, различни от изпълнението на договор със субекта на данните за доставка на стока или изпълнението на възмездна услуга, Администраторът не е задължен да получава съгласие на субекта на данните отделно от формата за индивидуализация на субекта на данните при сключване на договора. В този случай Администраторът събира единствено данните, които са му необходими за изпълнението на договора.

(2) За доставка на стоки чрез договор, сключван от разстояние, Администраторът събира единствено следните лични данни от субекта на данните:

- Трите имена на физическо лице;
- Единен граждански номер;

- Адрес за доставка на стоката;
- Имейл за обратна връзка;
- Данни за платежни средства;
- Телефонен номер за обратна връзка.

(3) За изпълнение на договор за услуга на информационното общество, Администраторът събира единствено следните лични данни от субекта на данните:

- Трите имена на физическо лице;
- Единен граждански номер;
- Адрес за изпращане на фактура, ако се издава в писмена форма;
- Имейл за обратна връзка;
- Данни за платежни средства;
- Телефонен номер за обратна връзка.

(4) В случай че Администраторът събира допълнителни лични данни, извън тези по ал. 2 и ал. 3, субектът на данните трябва да предостави изричното си съгласие по реда на този кодекс и GDPR. Това съгласие може да бъде дадено чрез формата за сключване на договора, но с отделен checkbox или бутон, в който изрично е посочена целта на обработката на личните данни и съгласието с тази цел. В този случай сключването на договора и неговото изпълнение трябва да е възможно и без субектът на данните да е дал съгласието за обработка на тези данни, които не са необходими за изпълнение на договора или ако е оттеглил това съгласие.

Чл. 7. (1) Администраторът има право да обработва лични данни, които са били събрани по реда на Закона за защита на личните данни, Директива 95/46/ЕС и преди 25 май 2018 г., само ако съгласието за събирането им е в съответствие с изискванията на GDPR и настоящия кодекс.

(2) В случай че съгласието за обработка не е получено от Администратора в съответствие с изискванията на ал. 1, Администраторът трябва да получи отново съгласието от всички субекти на данните по реда на този кодекс и GDPR.

Раздел III

Оттегляне на съгласието за обработка на лични данни

Чл. 8. (1) Оттеглянето на съгласието за обработка на лични данни от субекта на данните се извършва чрез попълване на предоставена от Администратора форма за оттегляне в профила на субекта на данните при Администратора, който е достъпен чрез форма от сайта на Администратора, услугата или приложението, за предоставянето на които е дадено съгласието.

(2) В случай на липса на функционалност за оттегляне на съгласието съгласно ал. 1 или ако Администраторът предоставя услуги без регистрация и създаване на профил, субектът на данните може да изпрати до Администратора по имейл или куриер попълнена форма за оттегляне на съгласие или искане в свободен текст.

(3) Администраторът продължава да предоставя услугата, приложението или функционалността на сайта, дори и след пълното или частично оттегляне на съгласието

за обработка на личните данни на субекта на данните, ако това е технически възможно и правно допустимо.

(4) Субектът на данните не може да оттегля съгласието за обработка на лични данни, които са необходими за изпълнение на задълженията на Администратора съгласно приложимото законодателство, като например следните данни:

- Счетоводна информация за индивидуализация на лицето за целите на запазване на данъчна информация;
- Информация, която е необходима на Администратора за защита на правата му при изпълнение на договора със субекта на данните, като например индивидуализация на лицето в съдебни процеси, административни производства или отправяне на претенции;
- Информация, която е необходима за доказване от Администратора на изпълнение на задълженията му по GDPR и този кодекс;
- Трафични данни за изпълнение на задълженията на Администратора съгласно Закона за електронните съобщения;
- Информация, която е необходима на Администратора за целите на сигурността, изпълнение на задълженията му към държавни органи, включително, но не само Министерство на вътрешните работи, Национална агенция по приходите и др.

(5) В случаите по ал. 4, Администраторът има право да обработва данните единствено за целите и на основанията, които са посочени в приложимото право.

(6) В случаите на оттегляне на съгласие от субекта на данните за обработката им и ако тези данни са необходими за предоставяне на услугата, счита се, че субектът на данните е изявил и прекратяване на предоставянето на услугата. В този случай Администраторът не носи отговорност за предоставянето на услугата след момента на получаване на оттеглянето.

(7) След оттегляне на съгласието от субекта на данните, Администраторът има право да ги обработва след анонимизирането им. В случай че след оттеглянето на съгласието Администраторът продължи обработката на личните данни на друго основание, Администраторът е задължен да уведоми за това субекта на данните.

(8) В случай на оттегляне на съгласие за обработка на данните, Администраторът съобщава на всички обработващи за оттеглянето на съгласието за обработка на тези данни за това лице. Администраторът не носи отговорност, в случай че обработващият, който е уведомен за оттеглянето на съгласието, продължи да обработва данните за различна цел.

(9) В случай че задължено лице по този кодекс действа в качеството си на Обработващ данните, оттеглянето на съгласието за обработка на данните има действие единствено по отношение на обработката на данните за конкретния администратор, който е възложил обработката на Обработващ данните, но не и по отношение на същите данни, които Обработващият обработва за други администратори.

(10) Администраторът може да използва за оттегляне на съгласието за обработка същите способи за доказване или верификация, както за получаване на съгласието за обработка на данните.

(11) Администраторът има право да запази изразеното съгласие и оттеглянето му, с оглед защита на интересите му при доказване, че същите са предоставени от субекта на данните.

Раздел IV

Информация, предоставяна от Администратора на субекта на данните

Чл. 9. Преди получаване на съгласието на субекта на данните и по всяко време докато обработва лични данни, Администраторът предоставя на субекта на данните следната информация:

1) Данни за идентификация на Администратора – наименование и ЕИК номер или БУЛСТАТ номер.
2) Целта на всяка една операция по обработка, за която се иска съгласие за обработка;
3) Какви категории данни ще се събират и използват;
4) Наличието на право на оттегляне на съгласието за обработка, както и всички права, с които субектът разполага по GDPR и начините за тяхното упражняване;
5) Информация за използването на данните за решения, основани изключително на автоматична обработка, включително профилиране в съответствие с чл. 22, ал. 2 от GDPR;
6) Ако съгласието се отнася за трансфер, за възможните рискове за трансфера на данни към трети държани при липсата на решение за адекватна защита и подходящи средства за защита;
7) Данни за контакт с Длъжностното лице по защита на данните, когато е приложимо.

Чл. 10. (1) При получаване на съгласието за обработка на данните и във всеки един момент след това, Администраторът предоставя на субекта на данните информацията по чл. 6 от този кодекс и чл. 13, ал. 1 от GDPR, както и следната информация:

a) Срока, за който ще се съхраняват личните данни, а ако това е възможно, критериите, използвани за определяне на този срок;
b) Съществуването на право да се иска от администратора достъп до, коригиране или попълване на, изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;
c) Когато обработването се основа на съгласието на субекта на данните, правото му да оттегли съгласието си по всяко време.
d) Правото на жалба до надзорен орган;
e) Дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключване на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

f) Съществуването на автоматизирано вземане на решения, включително профилиране и използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.
g) Източника на данните, и ако е приложимо, дали данните са от публично достъпен източник.

(2) Горната информация се предоставя от Администратора на субекта на данните по един от следните начини:

a) По имейл на посочен от субекта на данните адрес;
b) В електронна форма чрез главната страница на сайта на Администратора в Интернет или на услугата;
c) Privacy notice и/или Privacy policy, които присъстват в основната страница на домейна на услугата.

(3) В случай че Администраторът вече е предоставил горните данни, Администраторът може да не ги предоставя втори път на субекта на данните, освен ако иска съгласие за обработка на нови лични данни или за нови цели.

(4) Използването на образци за предоставяне на информация по този кодекс се счита за изпълнение на изискванията за предоставяне на информация по чл. 13 от GDPR.

Раздел V

Упражняване на правата от субектите на данните по GDPR

Чл. 11. (1) Във всеки един момент при упражняване на правата на субектите на данните, Администраторът има право да изисква от субекта на данните да представи доказателства, че същият е физическото лице, за което личните данни се отнасят.

(2) За удостоверяването на самоличността на субекта на данните при упражняване на правата му съгласно GDPR, Администраторът има право да приложи следните методи:

a) Универсален електронен подпис;
b) Карта за електронна идентификация;
c) Представяне на документ за самоличност от субекта на данните в офис на адрес, посочен от Администратора в града по седалището на Администратора или на друг адрес, посочен от Администратора като основен за упражняване на дейността му. В този случай Администраторът не събира и не обработва данните от документа за самоличност, а единствено удостоверява самоличността на лицето с цел упражняване на поисканото от него право.

(3) Счита се, че Администраторът е положил всички необходими усилия за защита на личните данни, ако от обстоятелства е видно, че лицето което извършва идентификацията е лицето, за което се отнасят личните данни, по отношение на които се упражняват правата по GDPR.

(4) Субектите на данните не могат да упражняват правата си по GDPR по начин, който нарушава сигурността на личните данни на други субекти, на информационната сигурност и на функционирането на услугите, предлагани от Администратора.

Право на корекция на личните данни

Чл. 12. (1) При упражняване на правото на корекция на личните данни съгласно чл. 16 от GDPR, субектът на данните не предоставя данни, които надхвърлят данните, които Администраторът е получил съгласие да събира.

(2) За събиране на допълнителни данни в случаите по ал. 1 по искане на Администратора, е необходимо субектът на данни да предостави изричното си съгласие относно новите данни и цели.

(3) Независимо от горното, в случай че субектът на данните по своя инициатива предостави чрез упражняване на правото си по чл. 16 от GDPR и допълнителни лични данни, които Администраторът не е обработвал до този момент, счита се с предоставянето им субектът на данните е предоставил и съгласието за обработката им от Администратора за същите цели.

Право на изтриване („право да бъдеш забравен“)

Чл. 13. (1) За целите на упражняване на правото да бъдеш забравен по чл. 17 от GDPR, под „без ненужно забавяне“ за Администратор по смисъла на този кодекс следва да се приема изпълнение на задължението на Администратора за изтриване в рамките на 10 работни дни, освен ако е необосновано трудно технически да се спази този срок, в който случай Администраторът полага усилия да изпълни задължението си най-късно до един месец след постъпване на искането от субекта.

(2) При упражняването на правото по ал. 1, субектът на данните е задължен да посочи уникален идентификатор, който да го идентифицира като субект на съответните лични данни, в съответствие с чл. 10 по-горе.

(3) В случай че лицето не е посочило уникален идентификатор по ал. 2, Администраторът има право да изисква такъв от субекта на данните, за целите на упражняване на правото, в съответствие с чл. 10 по-горе.

(4) Администраторът поддържа регистър на упражнените права по чл. 17 от GDPR само за целите на доказване, че е изпълнил задълженията си по чл. 17. В този регистър Администраторът съхранява единствено уникалния идентификатор на субекта на данните и категориите данни, които са били обект на правото по чл. 17 от GDPR, както и дата на постъпване на искането и дата на изтриване на данните.

(5) В случаите на упражняване на правата по чл. 17 от GDPR, Администраторът изтрива единствено личните данни на субекта, но не и публично достъпни публикации, които субектът на данните е направил във форуми, дискусионни панели, публикации и статии в сайт, чатове и други платформи, които са насочени към неограничен кръг лица. В този случай ако при публикацията са посочени лични данни, различни от името или потребителското име/nickname/username на публикуващия, Администраторът изтрива допълнителните данни в идентификацията на субекта на данните, ако това е технически възможно.

(6) При изпълнение на правото на отказ по чл. 17 от GDPR, Администраторът не изтрива обекти на интелектуална собственост, за които е придобил право да ги използва на правно основание.

(7) В случай на изтриване на данните на субекта при упражняване на правото му по чл. 17 от GDPR и в случай на последващо упражняване на правото на субекта по чл. 15 от GDPR за достъп, Администраторът му предоставя единствено информация, че съхранява данни и че субектът на данните е упражнил правото си да бъде забравен по чл. 17 от GDPR.

(8) При изпълнение на правото на изтриване по чл. 17 от GDPR, Администраторът не спира обработката на личните данни за субекта на данните, за които има задължение за обработка по силата на приложимото право. Такива лични данни са например уникален идентификатор или наименование за целите на данъчното законодателство, IP адрес, информация по Закона за електронните съобщения или за целите на защита правата на Администратора по гражданското законодателство или упражняването на административни права, или защита от незаконосъобразни актове на държавни органи.

(9) В случай на упражняване на правото по чл. 17 от GDPR от субекта на данните, Администраторът уведомява в срока по ал. 1 всички обработващи и/или администратори, на които той е предоставил същите данни за същото лице за обработка с посочване, че лицето за което данните се отнасят е упражнило правото си да бъде забравен съгласно чл. 17 от GDPR, освен ако това е невъзможно или изисква несъразмеримо големи усилия.

Право на преносимост на данните

Чл. 14. (1) При упражняване на правото на преносимост по чл. 20 от GDPR, Администраторите предоставят личните данни за съответния субект на данните във формат XML, JSON, CSV или друг одобрен от ИАБ Европа формат, с което се счита че са изпълнени изискванията за структуриран, широко използван и пригоден за четене машинен формат.

(2) В случаите по ал. 1, субектът на данните индивидуализира администратора, към когото следва да се извърши пренос на личните данни чрез уникален идентификатор от публично достъпен регистър съгласно приложимото право към съответния администратор и имейл адрес за изпращане на данните или API с необходимия достъп. Данните могат да се предоставят от Администратора и на оптичен или друг електронен носител на надлежно упълномощено или легитимирано лице по седалището на Администратора.

(3) Администраторите извършват преноса по ал. 2 в срок до 10 работни дни след идентифициране на субекта на данните и администратора към когото данните следва да се пренесат. В случай, че извършването на преноса е технически затруднено, Администраторът предава данните на посочения администратор в срок до един месец след идентифицирането му.

(4) В случаите по ал. 1, Администраторът не предоставя на третото лице данни, които са създадени от Администратора в процеса на предоставяне на услугата или в процеса на обработката и които не са изрично предоставени на Администратора от субекта на данните. На преносимост подлежат и посочените от субекта на данните псевдоними при използването на услугата или информацията.

(5) За целите на ал. 4, данните предоставени от субекта на данните, включват всички данни, които се отнасят до него или са резултат от наблюдаването на поведението на дадено физическо лице, но не включва данните, генерирани от последващия анализ на

това поведение. Всички данни, които са създадени от администратора на данни в рамките на обработването на данните (например категоризиране или профилиране), представляват производни или логически изведени данни от личните данни, предоставени от субекта на данните, и не са обхванати от правото на преносимост на данните.

(5) Администраторът отказва искане на субекта на данните за преносимост съгласно този член, ако субектът на данните вече е упражнил правото си да бъде забравен съгласно чл. 17 от GDPR.

(6) В случай че към Администратор е оправено искане за приемане на лични данни от субект на данните от друг администратор, Администраторът не е задължен да приема всички лични данни, които са предадени вследствие на искането за преносимост на данните, а само тези, които са необходими за предоставяне на услугата от приемащия Администратор. Новият получаващ Администратор е задължен да посочи явно и непосредствено целта на новото обработване при всяко искане за предаване на преносими данни съгласно GDPR, както и естеството на личните данни които са му необходими и релевантни за предоставянето на услугата на субекта на данните. В случай на упражнено от субекта на данните право на преносимост, се счита че той е дал съгласието си за тяхната обработка и съхранение от посочения от него получаващ администратор.

(7) В случаите по ал. 6, получаващият Администратор не може да използва или обработва пренесените лични данни, които се отнасят за трети лица, различни от субекта на данните, за свои собствени цели.

(8) Правото на преносимост на личните данни е приложимо единствено за лични данни, които Администраторът обработва по автоматизиран начин на следните основания:

a) получено съгласие от субекта на данните или
b) договор, по който субектът е страна;

(9) При получаване на данните от приемащия администратор, последният уведомява субекта на данните за правата му съгласно GDPR.

(10) Администраторът уведомява субектите на данните за възможността за преносимост на личните данни при закриване на потребителски акаунт при Администратора или при упражняване на правото да бъде забравен съгласно GDPR.

(11) Администраторите могат да използват потребителско име и парола за идентифициране на субекта на данните, който желае да упражни правото си на преносимост. По преценка на Администратора може да се изисква и допълнителна идентификация на субекта данните, включително присъствено представяне на документ за самоличност в офис на Администратора по седалището му.

(12) Ако предаването на данните по Интернет е проблемно с оглед обема на поисканите данни от страна на субекта на данните, Администраторът може да изиска от субекта на данните те да му бъдат предоставени чрез стрийминг или съхранение на CD, DVD или други физически носители, или директно към друг администратор на данни.

(13) Администраторът отговаря на искането по този член в срок до един месец от получаването му, като този срок може да бъде удължен до три месеца при сложни случаи, при условие че субектът на данните е бил уведомен относно причините за въпросното забавяне в рамките на един месец от получаване на първоначалното искане.

(14) Администраторът отговаря на искането на субекта на данните винаги, дори и да отговори с отказ. В случай на отказ от изпълнение на искането на субекта на данните по този член, Администраторът уведомява субекта на данните за причините да не предприеме действия и за възможността за подаване на жалба до Комисията за защита на личните данни и търсене на защита по съдебен ред не по-късно от един месец от получаването на искането за преносимост на данните.

(15) ИАБ България и Комисията за защита на личните данни могат да приемат стандарт за описание на личните данни с метаданни при преносимост, с оглед подобряване на оперативната съвместимост между Администраторите. При всички случаи на използване на метаданни, същите трябва да са достатъчни, за да се позволи функционирането и повторното използването на данните, но без да се разкриват търговски тайни.

Раздел VI

Съответствие с GDPR на администратори на лични данни

Чл. 14. (1) Придържането на Администратора към настоящия кодекс не е единствената гаранция за защита на личните данни на субектите на данните, но може да се използва като елемент за доказване на задълженията на администратора по GDPR.

(2) Когато Администраторът обработва лични данни съвместно с друг администратор или обработващ лични данни, Администраторът се задължава да получи съгласието на другия администратор с изискванията на този кодекс и на GDPR най-малко по отношение на съвместната обработка на личните данни.

Защита на данните на етапа на проектирането и по подразбиране

Чл. 15. Администраторът на лични данни съобразява специалните изисквания на този кодекс при изпълнение на задълженията си по чл. 25 от GDPR.

Раздел VII

Обработващ на личните данни

Чл. 16. (1) В случаите когато задълженото лице по този кодекс действа в качеството си на Обработващ лични данни, той осигурява спазването на изискванията на този кодекс, доколкото те могат да бъдат приложени съответно към него, в качеството му на обработващ.

(2) Във всички случаи по ал. 1, Обработващият данните уведомява Администратора, че има задължения да се придържа към настоящия кодекс, включително чрез посочване в договора му с Администратора.

(3) В случаите, когато Администраторът по този кодекс възлага обработката на данните на обработващ, който не е страна по този кодекс, Администраторът изисква от

обработващия да спазва изискванията на този кодекс, най-малко по отношение на предоставените му за обработка лични данни. Това задължение се включва и в договора за възлагане на обработка на личните данни между Администратора и обработващия.

(4) Администраторите и Обработващите лични данни осигуряват наличието в договорите си минимум на клаузите за защита, както са определени в Приложение № 6 към този кодекс.

(5) Преди приемане на възлагане на обработка на лични данни от Администратор, Обработващият изисква доказателство от Администратора, че последният е получил съгласието на субектите за обработката на техните данни посредством обработващ данните. В случай на получено общо съгласие за предоставяне на данните на обработващ, Обработващият изисква от Администратора да бъде посочен в списъка на обработващите лични данни, достъпен за субектите на данните на сайта на администратора.

Раздел VIII

Задължено лице по Кодекса

Определяне на качеството на задълженото лице

Чл. 17. (1) Задълженото лице по този кодекс може да действа като администратор или като обработващ лични данни, в зависимост от предлаганата услуга и информация, както следва:

a) Когато ползвателят на услугата или информацията възлага на Задълженото лице да обработва лични данни на трето лице за целите на използването на услугата или информацията, предоставяна от ползвателя, Задълженото лице действа в качеството на обработващ личните данни;

Пример: SaaS и Infrastructure as Service услуги, платформи за онлайн магазини, блог платформи, платформи за обмен на информация или форуми, облачни и хостинг услуги.

b) Когато ползвателят на услугата предоставя свои лични данни на Задълженото лице за целите на получаване на услуга, информация, продажба на стока или друга сделка, Задълженото лице действа в качеството на администратор, ако същото предоставя услугата от свое име и за своя сметка, а не по възлагане на трето лице.

Пример: Имейл услуги, новинарски сайтове с регистрация, онлайн игри, мобилни приложения за услуги, социални мрежи (с изключение на страници в социални мрежи), форуми, електронни магазини.

c) Когато Задълженото лице предоставя информация или услуга от името на трето лице и събира лични данни по възлагане на третото лице, Задълженото лице действа в качеството на обработващ лични данни по отношение на ползвателя на услугата или информацията.

Пример: Онлайн промоционални игри, томболи, кампании за събиране на информация, анкети, проучвания на потребителски нагласи, маркетингови проучвания.

(2) Ползвателят на услугата или информацията може да действа като администратор на лични данни или като обработващ данните, както следва:

a) В случаите, когато ползвателят определя целите и способите за обработка на личните данни, ползвателят на услугата действа като администратор, а Задълженото лице като обработващ данните;

Пример: SaaS и Infrastructure as Service услуги, платформи за онлайн магазини, блог платформи, платформи за обмен на информация или форуми.

b) В случаите, когато ползвателят на услугата обработва личните данни от името и съобразно инструкциите на трето лице, ползвателят действа като обработващ данните;

Пример: Управление на профили или услуги по възлагане на трето лице.

(3) В случаите по ал. 1, а), Задълженото лице действа единствено по инструкция на ползвателя на услугата и само доколкото може да има контрол върху личните данни, които ползвателят обработва. Договорът за използване на услугата и използването на нейните функции и възможности са направени достъпни от Задълженото лице като част от услугата представляват изчерпателно и изрично инструкциите на ползвателя на услугата към задълженото лице (доставчика на услугата). В този смисъл, Задълженото лице (доставчикът на услугата) няма контрол върху съдържанието и данните, които ползвателят на услугата избира да зареди в услугата (включително ако тези данни включват или не лични данни. В този случай Задълженото лице няма роля в процеса на взимане на решение дали ползвателят използва облачната инфраструктура за обработка на личните данни, за какви цели и дали същите са защитени. Съответно, отговорността на задълженото лице в този случай се ограничава до 1) съобразяване с инструкциите на ползвателя на услугата съгласно и както е описано в договора за предоставяне на услугата и 2) предоставянето на информация за услугата и функционалностите чрез нейния интерфейс. В случаите на предоставяне на хостинг услуги от Задълженото лице, последното няма контрол и няма отговорност за личните данни, които ползвателят на услугата обработва.

(4) В случаите по ал. 3, Задълженото лице и ползвателят на услугата сключват договор в писмена (електронна) форма по следния начин:

a) Единен договор;
b) Съвкупност от документи – базов договор с анекси към него за Services Level Agreement, договор за обработка на данни, политики за сигурност и други;
c) Стандартизирани общи условия, които се приемат онлайн;

(5) В случаите в които ползвателят на услугата или информацията има контрол върху способите за осигуряване на сигурност на лични данни, отговорността на Задълженото лице по този кодекс се ограничава единствено до надлежното предоставяне на услугата и нейната функционалност. Съответно, ползвателят на услугата е единствено отговорен за осигуряване на сигурността и защитата на личните данни при използването на услугата.

Задължени лица по този Кодекс

Чл. 18. (1) Задължено лице по този кодекс е:

a) Юридическо лице, което предлага услуги, свързани с дигиталния сектор и което е изразило съгласието си да се придържа към изискванията на този кодекс с декларация подадена до ИАБ България и получило ID;
b) Юридическо лице, което е член на ИАБ България и се е задължило пред ИАБ България да се съобразява с изискванията на този кодекс.

(2) Администратор по този кодекс е лице по ал. 1, което отговаря на изискванията на администратор по смисъла на GDPR.

Раздел IX

Сигурност и съответствие с GDPR при обработването на лични данни

Сигурност на обработването

Чл. 19. ИАБ България и КЗЛД приемат отделно от този кодекс минимални изисквания за сигурност при обработването, които след приемането им стават неразделна част от този кодекс и са задължителни за всички Администратори и Обработващи, към които кодексът се прилага.

Профилиране и автоматизирано взимане на решения

Чл. 20. (1) Администраторът взима изрично съгласие на субекта на данните за извършване на профилиране или автоматизирано вземане на решение въз основа на предоставените лични данни. В този случай Администраторът предоставя на субекта на данните следната информация:

a) Уведомление, че лицето участва в този вид дейност;
b) Информация за логиката на операцията в разбираема форма и
c) Обяснение за важността и предвижданите последици от обработката;
d) Наличието на автоматизирано взимане на решение за лицето, като се провежда такова;

(2) Администраторът не може да използва като основание за профилиране или автоматизирано взимане на решения съгласието на субекта на данните, ако услугата не може да се предостави без това съгласие. В този случай Администраторът сключва със субекта на данните договор в писмена форма, в който са описани условията и изискванията за извършване на профилиране или автоматизирано взимане на решения, но само ако изпълнението на договора изисква извършвана профилиране.

(3) В случай на упражняване на правото на достъп до лични данни, Администраторът ги предоставя в контекста на настоящия член, при опазване на търговската си тайна.

(4) Администраторът предоставя на субекта на данните отделно и различимо от другата информация по този кодекс, информация за правото на отказ на субекта на данните от автоматизирано взимане на решения и профилиране, посредством отделен попъп прозорец или раздел при извършване на регистрацията или използване на сайта му, или чрез изпращане на информацията по имейл на субекта на данните. Администраторът не

може да поставя условия за отказа на субекта на данните, когато извършва профилиране или автоматизирано взимане на решение за маркетингови цели.

(5) Администраторът извършва оценка на въздействието на всеки тип операция по профилиране и автоматизирано взимане на решение преди въвеждането й при Администратора.

(6) Администраторът прилага мерките по Annex 1 от Насоките относно Автоматизирано взимане на решения и Профилиране за целите на Регламент 2016/679.

Прозрачност при получаване на съгласието

Чл. 21. (1) Администраторът осигурява, че по всяко време от използването на сайта, който поддържа, субектът на данните има достъп до Политиката за защита за личните данни на Администратора чрез линк в долната или горната част на страницата с ясно означение Поверителност, Изявление за поверителност или Защита на личните данни или Privacy, Privacy Notice, Privacy Policy или Data Protection Notice, или чрез друга подходяща формулировка, която да е в достатъчна степен информативна за съдържанието си.

(2) В случай че Администраторът предоставя мобилно приложение на субекта на данните, основното меню на приложението съдържа линк към Политиката за защита на личните данни и функционалност за изменение на настройките за защита на личните данни.

(3) При всички случаи, информацията за правата на субекта по този кодекс и GDPR се предоставя на същата страница, чрез която се събират личните данни.

(4) При получаване на съгласието за обработка личните данни, Администраторът посочва явно и конкретно (а не общо и генерално) целите, за които се събират и предоставя информацията на ясен и разбираем език, без да използва условни изрази.

(5) В случаите на събиране на личните данни от субекта на данните, Администраторът предоставя изискуемата информация в момента на събирането на данните. В случай че данните не се събират от субекта на данните, Администраторът предоставя изискуемата информация в разумен срок, но не по-късно от 1 месец от събирането й, ако Администраторът може да идентифицира субекта на данните по начин, който позволява осъществяване на контакт с лицето.

(6) Администраторът предоставя информацията по този кодекс и възможност на субекта на данните за промяна на настройките за поверителност чрез единен административен панел за управление, достъпен в сайта или приложението на Администратора.

Оценка на въздействието

Чл. 22. (1) Оценката на въздействието на защита на личните данни представлява процес, чиято цел е да се опише обработването, да се оцени неговата необходимост и пропорционалност и да се спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове.

(2) Администраторите извършват оценка на въздействието на обработките на лични данни с оглед осигуряване на сигурност и демонстрация на съответствие с GDPR.

(3) Администраторите извършват оценка на въздействието на защита на личните данни, само когато съществува вероятност обработването да породи висок риск за правата и свободите на физическите лица. В случаите в които има колебание дали определена операция подлежи на оценка на въздействието на защита на личните данни, Администраторът извършва оценката на въздействието.

(4) За следните операции с лични данни не се изисква извършване на оценка на въздействието на защита на личните данни:

- Обработка на лични данни за целите на създаване на профил във форум или друга дискусионна платформа, ако личните данни не се използват за никакви други цели;
- Обработка на лични данни за целите на изпълнение на договор за продажба на стоки от разстояние, ако личните данни не се използват за никакви други цели;
- Обработка на лични данни за целите на предоставяне на услуга на информационното общество, ако събираните лични данни са единствено за индивидуализация на лицето като страна по договора, данни за осъществяване на контакт, имейл и профил в социални мрежи;
- Обработка на лични данни за целите на създаване на профил за използване на приложение или услуга в сайт, ако данните са минимално необходимите за предоставяне на услугата и не се извършва профилиране или автоматизирано взимане на решения за субекта на данните;
- Обработка на лични данни за целите на участие в томболи, състезания и игри, ако се събират лични данни само за индивидуализация на участващите лица и осъществяване на контакт с тях;
- Обработка на данни за маркетингови и социологически проучвания, ако данните се събират като псевдонимизирани или аномизирани, без да разкриват данни за физическото лице.

(5) Оценката на въздействието на защита на личните данни подлежи на постоянно преразглеждане и преоценка от Администраторът най-малко веднъж на всеки 12 месеца.

(6) Администраторът извършва оценка на въздействието на защита на личните данни на възможно най-ранния етап от проектирането на операцията по обработка.

(7) Администраторът публикува заедно с другата информация по този кодекс, резюме или заключението на резултатите от оценка на въздействието на защита на личните данни за отделните операции по обработка.

Длъжностно лице за защита на личните данни

Чл. 23. Администраторът може по свой избор използва Длъжностно лице за защита на личните данни за изпълнение на задълженията си по GDPR и този кодекс, освен ако това не е задължително съгласно чл. 37 (1) от GDPR.

Знак за съответствие

Чл. 24. Задължените по този кодекс лица задължително поставят знак за съответствие с изискванията на този кодекс и линк към него, съгласно приетите от Управителния съвет на ИАБ България изисквания към знака, неговото изобразяване и поставяне.

Уведомяване на Комисията за защита на личните данни и субектите на данни при нарушение на сигурността

Чл. 25. (1) В случай, че Администраторът установи нарушение на сигурността на личните данни, той изпраща до Комисия за защита на личните данни уведомление за нарушението не по-късно от 72 часа след като е разбрал за него, освен ако не съществува вероятност нарушението на сигурността на данните да породи риск за правата и свободите на физическите лица.

(2) В случай, че Администраторът установи нарушение на сигурността на личните данни, което би могло да породи висок риск за правата на физическите лица, Администраторът уведомява субекта на данните не по-късно от 72 часа от установяване на вероятността за пораждане на висок риск.

Чл. 26. В случай, че след извършване на оценка на въздействието върху защитата на данните, Администраторът установи, че обработването би могло да породи висок риск, Администраторът по своя преценка може да се консултира с Комисията за защита на личните данни.

Чл. 27. За целите на член 25 и 26, „висок риск“ е по-вероятно да се породи в един от следните случаи, за което Администраторът осъществява контрол и проверка:

1. профилиране и прогнозиране на данни, отнасящи се до икономическото състояние, здравето, личните предпочитания и интереси, поведението или местоположението на субекта на данни;

2. автоматизирано вземане на решения, от което биха произтекли съществени правни последици за субекта на данните;

3. обработване на специални категории лични данни на над 10 000 физически лица;

4. мащабно обработване на лични данни, което включва обработката на данни на над 10 000 физически лица или за неограничен период на съхранение;

5. обработване на лични данни на субекти, които се нуждаят от по-високо ниво на защита (напр. деца под 16 г., лица с психични заболявания, възрастни лица над 75 години и др.);

6. използване на нови технологии за идентификация и събиране на данни на физическите лица;

7. обработване, което би довело до ограничаване на правото на субекта на данните да упражни правата си или да се ползва от предоставяната услуга.

Разрешаване на спорове

Чл. 28. (1) Всички спорове между Администратори или между Администратор и субект на данните могат да бъдат отнасяни за разрешаване към Комисията за защита на личните данни.

(2) Споровете между Администратори и субекти на данните относно обезщетения за вреди се разрешават доброволно чрез преговори между страните, като ако не постигнат съгласие, се разрешават от компетентните български съдилища.

Този кодекс е изготвен от ИАБ България на основание чл. 40, ал. 2 от GDPR и влиза в сила след одобрението му от Комисията за защита на личните данни съгласно чл. 40, ал. 5 от GDPR.

Приложение № 1 – Примерни форми за изразяване на съгласие за целите на обработка

[Индивидуализация на лицето]

[Индивидуализация на администратора]

Форма за даване на съгласие за обработване на лични данни, предоставени от лице над 16 години

☒Съгласен/съгласна съм предоставените от мен лични данни да бъдат събирани, обработвани и съхранявани от …… за следните цели:

Тип лични данни …….. [например Име] за следните цели:

☐За предоставяне на услугата и осигуряване на нейната пълна функционалност

☐За завършване на регистрацията в уебсайта и предоставяне на потребителски профил

☐За изпращане на нюслетъри и други рекламни съобщения

☐Всички

Тип лични данни …….. [например адрес] за следните цели:

☐За предоставяне на услугата и осигуряване на нейната пълна функционалност

☐За завършване на регистрацията в уебсайта и предоставяне на потребителски профил

☐За изпращане на нюслетъри и други рекламни съобщения

☒Всички

……. Продължава за всеки тип лични данни

Ако сте под 16 години, моля кликнете тук.

Форма за даване на съгласие за обработване на лични данни, предоставени от лице под 16 години.

☐Съгласен/съгласна съм личните данни, предоставени от моето дете, да бъдат събирани, обработвани и съхранявани от …… за следните цели:

Тип лични данни …….. [например Име] за следните цели:

☐За предоставяне на услугата и осигуряване на нейната пълна функционалност

☐За завършване на регистрацията в уебсайта и предоставяне на потребителски профил

☐За изпращане на нюслетъри и други рекламни съобщения

☐Всички

Приложение № 2 – Примерни форми за оттегляне на съгласие за целите на обработка

[Индивидуализация на лицето]

[Индивидуализация на администратора]

☐Оттеглям съгласието си за събиране, обработване и съхранение на следните лични данни, предоставени от мен:

☐Всички предоставени от мен лични данни

☐Име

☐ЕГН

☐Адрес

☐Телефон

☐Имейл

☐Данни за платежни средства

за следните цели:

☐За предоставяне на услугата и осигуряване на нейната пълна функционалност

☐За завършване на регистрацията в уебсайта и предоставяне на потребителски профил

☐За изпращане на нюслетъри и други рекламни съобщения

☐Всички

☐Декларирам, че съм запознат с условията на администратора за предоставяне на услугата след оттегляне на съгласието.

Приложение № 3 – Искане „да бъда забравен“ - за изтриване на личните данни, свързани с мен

[Индивидуализация на администратора]

Три имена
ЕГН
Номер на документ за самоличност
Телефон
E-mail
Потребителско име

Моля всички лични данни, които събирате, обработвате и съхранявате, предоставени от мен или от трети лица, които са свързани с мен, съобразно посочената идентификация, да бъдат изтрити от Вашите бази данни.

Декларирам, че ми е известно, че част или всички от личните ми данни могат да продължат да бъдат обработвани и съхранявани от администратора за целите на изпълнение на законовите му задължения.

Приложение № 4 – Искане за преносимост на лични данни

[Индивидуализация на администратора]

Три имена
ЕГН
Номер на документ за самоличност
Телефон
E-mail
Потребителско име

Моля всички свързани с мен лични данни, които се събират, обработват и съхраняват във Вашите бази данни, да бъдат изпратени на:

☐e-mail: ____

☐Администратор – приемащ данните:

Наименование
Идентификационен номер (ЕИК, БУЛСТАТ, рег. номер в КЗЛД)
E-mail
API адрес

Моля личните ми данни да бъдат предадени в следния формат:

☐XML

☐JSON

☐CSV

☐Друг: ____

Желая лични ми данни в избрания формат да бъдат предадени на мен/ на посочения от мен администратор:

☐На посочения e-mail или чрез API ……..

☐На физически оптичен или електронен носител (CD, DVD, USB) на Вашия адрес

Приложение № 5 – Изявление за поверителност (Privacy notice)

Информация относно Администратора на лични данни

Наименование
ЕИК/БУЛСТАТ
Седалище и адрес на управление
Адрес за кореспонденция
Телефон
E-mail
Регистрация на администратор на лични данни в КЗЛД

Информация относно длъжностното лице по защита на личните данни

Наименование
ЕИК/БУЛСТАТ
Седалище и адрес на управление
Адрес за кореспонденция
Телефон
E-mail

Информация относно компетентния надзорен орган

Наименование	**Комисия за защита на личните данни**
Седалище и адрес на управление	**гр. София 1592, бул. „Проф. Цветан Лазаров” № 2**
Адрес за кореспонденция	**гр. София 1592, бул. „Проф. Цветан Лазаров” № 2**
Телефон	**02 915 3 518**
Интернет страница	**www.cpdp.bg**

„……“ осъществява дейността си в съответствие със Закона за защита на личните данни и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

Основание за събиране, обработване и съхраняване на вашите лични данни

Чл. 1. Администраторът събира и обработва Вашите лични данни на основание чл. 6, ал. 1, Регламент (ЕС) 2016/679, и по-конкретно въз основа на следното:

- Изрично получено съгласие от Вас като ползвател на услугата/клиент;
- Изпълнение на задълженията на Администратора по договор с Вас;
- Спазване на законово задължение, което се прилага спрямо Администратора;
- Защита на жизненоважни интереси на Вас или на друго физическо лице;
- Изпълнение на задача от обществен интерес или при упражняването на официални правомощия на Администратора;
- За целите на легитимните интереси на Администратора или на трета страна.

Цели и принципи при събирането, обработването и съхраняването на вашите лични данни

Чл. 2. (1) Администраторът събира и обработва личните данни, които Вие ни предоставяте, за целите на изпълнение на задълженията по договора, включително за следните цели:

- счетоводни цели;
- статистически цели;
- защита на информационната сигурност;
- обезпечаване на изпълнението на договора за предоставяне на съответната услуга;
- разрешаване на спорове между Вас и трети лица.

(2) Администраторът спазва следните принципи при обработката на Вашите лични данни:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите на обработване;
- съотносимост с целите на обработката и свеждане до минимум на събираните данни;
- точност и актуалност на данните;
- ограничение на съхранението с оглед постигане на целите;
- цялостност и поверителност на обработването и гарантиране на подходящо ниво на сигурност на личните данни.

(3) При обработването и съхранението на личните данни, Администраторът може да обработва и съхранява личните данни с цел защита следните си легитимни интереси:

- изпълнение на задълженията си към Национална агенция по приходите, Министерство на вътрешните работи и други държавни и общински органи.

Какви видове лични данни събира, обработва и съхранява администраторът?

Чл. 3. (1) Администраторът извършва следните операции с личните данни за следните цели:

- създаване на профил за използване на услугата – целта на тази операция е идентифициране на лицето, за да му бъде предоставена услугата;
- обработка на плащане за услуга и счетоводно отчитане – целта на тази операция е осигуряване на възможност за извършване на плащане и водене на счетоводството;
- обработка на поръчка на стока – целта на тази операция е приемане на поръчка и доставка на стоката от електронен магазин до краен клиент;
- *[описание на операция] – [описание на целта на операцията]*

(2) Администраторът обработва следните категории лични данни и информация за следните цели:

- Ваши индивидуализиращи данни (напр. име, ЕГН, адрес, електронна поща и др.) – за целите на ……..
- вид и срок на използваните от Вас услуги -– за целите на ……..
- стойност на използваните услуги за съответния срок – за целите на ……..;
- информация, свързана с плащане и избраните методи на плащане– за целите на …….. ;
- други данни, необходими за изпълнението на задълженията по договора – за целите на ……...

(2) Администраторът не събира и не обработва лични данни, които се отнасят за следното:

- разкриват расов или етнически произход;
- разкриват политически, религиозни или философски убеждения, или членство в синдикални организации;
- генетични и биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация.

(3) Администраторът обработва специалните категории данни по ал. 2 съгласно едно или повече от следните основания:

☐Изрично предоставено от Вас съгласие;

☐Изискване на трудовото право и правото в областта на социалната сигурност и закрила;

☐Обработването е необходимо за защита на жизненоважни интереси на Вас или друго физическо лице, когато е налице физическа или юридическа неспособност Вие да дадете лично съгласието си;

☐Обработването е свързано с дейността на фондация, сдружение или друго юридическо лице с нестопанска цел, с политическа, философска, религиозна или синдикална цел, ако обработването е свързано с членовете или бившите членове на тази структура, или лица, поддържащи връзка с тях, с Ваше съгласие;

☐Вие сте направили данните си обществено достояние;

☐Обработването е необходимо с цел установяване, упражняване или защита на правни претенции или при изпълнение на функциите на съдилищата;

☐Налице е важен обществен интерес на основание правото на ЕС или правото на държава-членка;

☐Обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинска диагноза, осигуряване на здравни или социални грижи или лечение, за целите на управлението на услугите и системите за здравеопазване или социални грижи, или съгласно договор с медицинско лице;

☐Обработването е необходимо от съображения от обществен интерес в областта на общественото здраве;

☐Обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания, или за статистически цели.

(4) Личните данни са събрание от Администратора от следните източници:

- ……..

Срок на съхранение на личните ви данни

Чл. 4. (1) Администраторът съхранява Вашите лични данни за срок не по-дълъг от …….. След изтичането на този срок, Администраторът полага необходимите грижи да изтрие и унищожи всички Ваши данни, без ненужно забавяне.

(2) Администраторът Ви уведомява, в случай, че срокът за съхранение на данните е необходимо да бъде удължен с оглед изпълнение на целите, изпълнение на договора, с оглед легитимни интереси на Администратора или друго.

Предаване на вашите лични данни за обработване

Чл. 5. (1) Администраторът може по собствена преценка да предава част или всички Ваши лични данни на обработващи лични данни за изпълнението на целите за обработване при спазване на изискванията на Регламент (ЕС) 2016/679.

(2) Администраторът Ви уведомява в случай на намерение да предаде част или всички Ваши лични данни на трети държави или международни организации.

Вашите права при събирането, обработването и съхранението на личните ви данни

Право на достъп

Чл. 6. (1) Вие имате право да изискате и получите от Администратора потвърждение дали се обработват лични данни, свързани с Вас.

(2) Вие имате право да получите достъп до данните, свързани с него, както и до информацията, отнасяща се до събирането, обработването и съхранението на личните Ви данни.

(3) Администраторът Ви предоставя при поискване, копие от обработваните лични данни, свързани с Вас, в електронна или друга подходяща форма.

(4) Предоставянето на достъп до данните е безплатно, но Администраторът си запазва правото да наложи административна такса, в случай на повторяемост или прекомерност на исканията.

Право на коригиране или попълване

Чл. 7. Вие имате право да поискате от Администратора да:

- коригира неточните лични данни, свързани с Вас;
- да попълни непълните лични данни, свързани с Вас.

Право на изтриване („да бъдеш забравен“)

Чл. 8. (1) Вие имате правото да поискате от Администратора изтриване на свързаните с Вас лични данни, а Администраторът има задължението да ги изтрие без ненужно забавяне, когато е налице някое от посочените по-долу основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- Вие оттеглите своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;
- Вие възразите срещу обработването на свързаните с Вас лични данни, включително за целите на директния маркетинг и няма законни основания за обработването, които да имат преимущество;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо Администратора;
- личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

(2) Администраторът не е длъжен да изтрие личните данни, ако ги съхранява и обработва:

- за упражняване на правото на свобода на изразяването и правото на информация;
- за спазване на правно задължение, което изисква обработване, предвидено в правото на ЕС или правото на държавата членка, което се прилага спрямо Администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са му предоставени;
- по причини от обществен интерес в областта на общественото здраве;
- за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
- за установяването, упражняването или защитата на правни претенции.

Право на ограничаване

Чл. 9. Вие имате право да изискате от Администратора да ограничи обработването на свързаните с Вас данни, когато:

- оспорите точността на личните данни, за срок, който позволява на Администратора да провери точността на личните данни;
- обработването е неправомерно, но Вие не желаете личните данни да бъдат изтрити, а само използването им да бъде ограничено;
- Администраторът не се нуждае повече от личните данни за целите на обработването, но Вие ги изисквате за установяването, упражняването или защитата на свои правни претенции;
- Възразили сте срещу обработването в очакване на проверка дали законните основания на Администратора имат преимущество пред Вашите интереси.

Право на преносимост

Чл. 10. Ако сте дали съгласие за обработване на Вашите лични данни или обработването е необходимо за изпълнението на договора с Администратора, или ако данните Ви се обработват по автоматизиран начин, Вие можете, след като се легитимирате пред Администратора:

- да поискате от Администратора да Ви предостави Вашите лични данни в четим формат и да ги прехвърлите към друг Администратор;
- да поискате от Администратора пряко да прехвърли Вашите лични данни към посочен от Вас администратор, когато това е технически осъществимо.

Право на получаване на информация

Чл. 11. Вие можете да поискате от Администратора да Ви информира относно всички получатели, на които личните данни, за които е поискано коригиране, изтриване или ограничаване на обработването, са били разкрити. Администраторът може да откаже да предостави тази информация, ако това би било невъзможно или изисква несъразмерно големи усилия.

Право на възражение

Чл. 12. Вие можете да възразите по всяко време срещу обработването на лични данни от Администратора, които се отнасят до него, включително ако се обработват за целите на профилиране или директен маркетинг.

Вашите права при нарушение на сигурността на личните ви данни

Чл. 13. (1) Ако Администраторът установи нарушение на сигурността на личните Ви данни, което може да породи висок риск за Вашите права и свободи, той Ви уведомява без ненужно забавяне за нарушението, както и за мерките, които са предприети или предстои да бъдат предприети.

(2) Администраторът не е длъжен да Ви уведомява, ако:

- е предприел подходящи технически и организационни мерки за защита по отношение на данните, засегнати от нарушението на сигурността;
- е взел впоследствие мерки, които гарантират, че нарушението няма да доведе до висок риск за правата Ви;
- уведомяването би изисквало непропорционални усилия.

Лица, на които се предоставят личните ви данни

Чл. 14. За целите на обработване на личните Ви данни и предоставяне на услугата, Администраторът може да предостави данните на следните лица, които са обработващи данни:

- ……;
- ……;

Посочените обработващи лични данни спазват всички изисквания за законност и сигурност при обработването и съхраняването на личните Ви данни.

Чл. 15. *Ако съгласието се отнася за трансфер, Администраторът описва възможните рискове за трансфера на данните към трети държави при липсата на решение за адекватна защита и подходящи средства за защита*.

Приложение № 6 – Примерни договорни клаузи в договори на администратор и обработващ данните

За целите на изпълнение на изискванията по този Кодекс, задължените лица включват в договорите си с трети лица следните клаузи:

1. Администратори - Администраторите включват в договорите си с доставчици, на които възлагат обработката на лични данни следните клаузи:

„(1) [*Задълженото лице*] възлага на доставчика обработката на лични данни от категориите и за изпълнение на целите, определени в Приложение към този договор.

(2) [*Задълженото лице*] спазва изискванията съгласно GDPR и е задължено лице по Кодекса за защита на личните данни на ИАБ България, достъпен на адрес ……., който се счита за неразделна част от този договор

(3) Доставчикът се задължава при обработката на личните данни по ал. 1 да спазва изискванията съгласно GDPR и Кодекса за защита на личните данни на ИАБ България, достъпен на адрес ……., който се счита за неразделна част от този договор.“

2. Обработващи – Обработващите данни включват в договорите с администраторите, които им възлагат обработка на данните следните клаузи:

„(1) [*Задълженото лице*] приема от възложителя обработката на лични данни от категориите и за изпълнение на целите, определени в Приложение към този договор.

(2) [*Задълженото лице*] се е задължило при обработката на личните данни по ал. 1 да спазва изискванията съгласно GDPR и Кодекса за защита на личните данни на ИАБ България, достъпен на адрес ……., който се счита за неразделна част от този договор.

(3) Възложителят се задължава и декларира, че е получил съгласието на субектите на данните, личните им данни да бъдат предоставени за обработка на [*Задълженото лице*].

(4) Възложителят декларира и се задължава, че спазва изискванията на GDPR за обработка на личните данни, които предоставя за обработка на [*Задълженото лице*].“