БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО ИНЖЕНЕРНА ХИМИЯ

тел.: (+359 2) 979 3288 e-mail: office@iche.bas.bg

ул. „Акад. Г. Бончев", бл. 103, 1113, София

ВЪТРЕШНИ ПРАВИЛА ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ И ЗА ДОПУСТИМИЯ ВИД ЗАЩИТА НА ЛИЧНИ ДАННИ

в Институт по инженерна химия

съгласно Регламент 2016/679

(Съгласно ЗЗЛД 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 и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

• *Регламент (ЕС) 2016/679 е обнародван в Официален вестник на Европейския съюз от 04.05.2016 г.*
• *Регламентът ще се прилага пряко във всички държави-членки от 25 май 2018 г.*

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите вътрешни правила уреждат условията и реда за водене на регистри по Закона за защита на личните данни (ЗЗЛД), както и организацията и реда за упражняване на контрол при обработването на лични данни от служителите на Институт по инженерна химия /ИИХ/.

(2) По смисъла на настоящите правила и Закона за защита на личните данни обработване на личните данни е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.
(3) Обработване на личните данни в ИИХ се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

Чл. 2. (1) Вътрешните правила се приемат с цел да регламентират:
1. създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно

обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
2. видовете регистри, които се водят в ИИХ и тяхното описание.
3. необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).
4. правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.
5. процедури за докладване, управляване и реагиране при инциденти.

(2) Вътрешните правила се утвърждават, допълват, изменят и отменят от Директора на ИИХ.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и се издават на основание чл.13, ал.1 от Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.

Чл. 4. ИИХ е администратор на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни.

Чл. 5. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.
(2) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

II. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 6. (1) Администраторът възлага обработването на личните данни на негови служители (обработващи). Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.
(2) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

Чл. 7. (1) Личните данни в регистрите се набират от администратора на лични данни респективно - обработващият лични данни чрез устно интервю и/или на хартиен носител.
(2) За необходимостта от набирането на данните и целите, за които ще бъдат използвани, обработващият данните информира лицето, след което се съхранява на хартиен носител. (3) За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.
(4) Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки в определени шкафове и не се изнасят от сградата на ИИХ, освен от обработващия лични данни, при служебна необходимост и на технически носител като периодично обработващия лични данни ги архивира.

III. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ

Чл. 8. Форма на организация и съхраняване на личните данни на хартиен носител:
(1) Папките са разположени върху работните бюра и в офис шкафове в кабинета на зав. Административно стопанска дейност, които се заключват. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри се контролира от ИИХ.
(2) Местонахождение на картотечния шкаф - може да бъде поставен в помещение, предназначено за самостоятелна работа на обработващия лични данни или в общо помещение за работа с изпълняващи други дейности.
(3) Носител (форма) за предоставяне на данните от физическите лица - личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез:
- устно интервю с лицето;
- хартиен носител - писмени документи (заявления) по текущи въпроси в процеса на работа, подадени от лицето;
- външни източници (съдебни, финансови, осигурителни, данъчни и др. институции в изпълнение на нормативни изисквания).
(4) Личните данни от лицата се подават до администратора на личните данни - ИИХ., представляван от директора на ИИХ и длъжностното лице, определено за обработване на лични данни със заповед на директора на образователната институция.
(5) Възможността за предоставяне другиму достъп до личните данни при обработката им е ограничена и изрично е регламентирана в Раздел VI на настоящите Вътрешни правила.

Чл. 9. Форма на организация и съхраняване на личните данни от ИИХ на технически носител:
(1) Личните данни се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни и мерки при средно ниво, съобразно изискванията на Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.
(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.
(3) Достъп до файловете за обработка на лични данни имат само работещите с нея.
(4) Местонахождение на сървъра - съобразно изискванията на Вътрешни правила за информационните системи в ИИХ. местонахождение на компютрите - в изолирано помещение за самостоятелна работа на обработващия лични данни по регистъра, и в общо помещение с изпълняващи други дейности без право на достъп до него на останалите служители. Правото на достъп е регламентирано в специално изготвени декларации.
(5) Достъп до файловете за обработка на лични данни има само определено със заповед на директора лице обработващо лични данни.
(6) Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на електронни носители, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва от отговорен служител Боян Бояджиев. Когато данните се намират на изолирани компютри

архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

IV. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

Чл. 10. (1) Програмно-апаратни мерки за гарантиране нивото на сигурност:
- компютърните сървъри за база данни на ниво образователна институция да са на съвременно техническо ниво.
- компютърните работни конфигурации използват Desktop операционни системи, съобразно изискванията на приложния софтуер за работа с лични данни.
(2) За всички отговорни компютърни конфигурации и сървъри, от които зависи правилното поддържане на базите с лични данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).
(3) Минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва:
- съвременна Desktop операционна система съобразно изискванията на ползвания приложен софтуер;
- антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
- активирана защитна стена предотвратяваща идентифициране на IP адрес на потребителя и достъп на злонамерен софтуер до компютрите.
(4) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се контролира съобразно изискванията на Вътрешни правила за информационните системи в ИИХ

Чл. 11. Физически мерки за гарантиране нивото на сигурност:
(1) В помещенията, в които са разположени компютърни и комуникационни средства, следва да се осигури:
- всички работни помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран.
- всички носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват от обработващите лични данни. Контролът по използването на тези носители се извършва от директора.

Чл. 12. Организационни мерки за гарантиране нивото на сигурност:
(1) Организира се охрана на работните помещения в рамките на охраната на цялата сграда.
(2) Работата с информационните системи се организира съобразно Вътрешни правила за информационните системи в ИИХ.
(3) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
(4) Проверка на всички работни компютърни конфигурации по чл. 5, ал. 1, т. 10 от Наредбата за минималното ниво на техническите и организационни мерки и допустимия вид защита на личните данни се извършва периодично от ИИХ.
(5) Пренасянето на лични данни през интернет се осъществява чрез електронна поща.
(6) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.
(7) Със заповед директора на ИИХ се определят обработващите лични данни за различните видове регистри, които се водят в института.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 13. Служителите от ИИХ са длъжни да спазват и изпълняват настоящите вътрешни правила, в съответствие с длъжностните им характеристики.

Чл. 14. При обработване на личните данни служителят подписва декларация, че е запознат с изискванията за защита на личните данни, инструкцията относно механизма на обработване на лични данни и защитата им от незаконни форми на обработване, както и с настоящите вътрешни правила.

Чл. 15. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.
(2) Лични данни се предоставят служебно между структурните звена и служителите на ИИХ след обосновано искане, чрез докладна записка.

Чл. 16. (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани в ИИХ
(2) Правото на достъп се осъществява с писмено заявление/или заявление по електронен път, подадено по реда на Закона за електронните документи и електронния подпис, до директора на образователната институция лично или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно. Подаването на заявлението е безплатно.
(3) Заявлението съдържа:
- име, адрес и други данни за идентифициране на съответното физическо лице;
- описание на искането;
- предпочитана форма за предоставяне на информацията;
- подпис, дата на подаване на заявлението и адрес за кореспонденция;
- приложено пълномощно, когато заявлението се подава от упълномощено лице.
(4) Заявлението се завежда в деловодството на ИИХ.
(5) Достъп до данните на лицето се осигурява под формата на:
- устна справка;
- писмена справка;
- преглед на данните от самото лице или от упълномощеното такова;
- копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.
(6) При подаване на заявление за осигуряване на достъп до лични данни, Дирикторът разглежда заявленията и разпорежда на обработващия лични данни да осигури искания достъп от лицето в предпочитаната от него форма.
(7) Срокът за разглеждане на заявлението и произнасянето по него е 14-дневен от деня на подаването му. Срокът може да бъде мотивирано удължен до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.
(8) Директорът уведомява писмено заявителя за решението си - то може да бъде за предоставяне на достъп или отказ за достъп. Уведомяването става лично срещу подпис или по пощата с обратна разписка.
(9) Отказът на достъп до лични данни трябва да бъде мотивиран, а основанията за отказ са:
- когато данните не съществуват;
- когато данните не могат да бъдат предоставяни на определено правно основание.
(10) За отказ се счита и липсата на уведомление.
(11) Отказът за предоставяне на достъп до лични данни може да се обжалва от лицето в съда.
(12) Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на директора - обработващ лични данни, който чрез парола има

достъп до информацията и до съответния компютър.
(13) Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите на лицата, отговарящи за съответната дейност, за която се водят регистри. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

Чл. 17. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.
(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.
(3) Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.
(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице Директорът съобщава на третото лице в 30-дневен срок от подаване на искането.

VI. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ,
УПРАВЛЯНИЕ И РЕАКЦИЯ ПРИ ИНЦИДЕНТИ

Чл. 18. (1) При възникване и установяване на инцидент незабавно се докладва на лицето, отговорно за защита на личните данни.
(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.
(3) След анализ от зав. Административно стопанска дейност на ИИХ в дневника се записват последствията от инцидента и мерките, които са предприети за отстраняването им.
(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.
(5) В случаите на компрометирането на парола тя се подменя с нова, като събитието се отразява в дневника за инциденти.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящите Вътрешни правила:
§1. „Администратор на лични данни” е ИИХ. представлявано от директора на института.
§2. „Обработващ лични данни” са длъжностни лица от ИИХ, определени със заповед от директора на ИИХ
§3. Вътрешните правила влизат в сила от деня на тяхното утвърждаване.
§4. Настоящите Вътрешни правила за минимално ниво на технически и организационни мерки и за допустимия вид защита на лични данни, са приети и утвърдени на ИИХ, от директора на ИИХ.