ИНСТРУКЦИЯ ОТНОСНО НЕОБХОДИМИТЕ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В СЪЮЗА НА УЧЕНИТЕ В БЪЛГАРИЯ

1. Настоящата инструкция регламентира правомерното обработване на лични данни от СУБ в качеството му на администратор на лични данни (АДМИНИСТРАТОР), както и от определените да изпълняват функциите на обработващ лични данни служители (ОБРАБОТВАЩ/И), във връзка с въвеждане на новите нормативни изисквания в областта на защита на личните данни – Регламент 2016/679, Закон за защита на личните данни и подзаконовите актове за прилагането му, ръководствата и насоките на КЗЛД и Работната група по чл. 29 (след 25.05.2018 г. – Европейския комитет по защита на данните).

2. ОБРАБОТВАЩИ личните данни в СУБ от името на администратора са служители, на които това задължение е възложено с правен акт – трудов договор и длъжностна характеристика. В СУБ това са (с различно ниво на достъп - пълен, конкретизиран и ограничен): Председателят на Управителния съвет на СУБ или определен с негова заповед заместник в предвидените за такова заместване случаи; служителите във финансово-счетоводното звено; експертът в отдел „Секции и клонове“

3. ОБРАБОТВАЩИЯТ лични данни се задължава да предприеме необходимите технически и организационни мерки за защита на предоставените му лични данни, като се съобразява със съвременните технологични постижения и спецификите на дейността си и осигурява ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени. Тези задължения на обработващите лични данни се вписват в техните длъжностни характеристики.

4. Лични данни са всяка информация, отнасяща се до физическо лице, чрез която то може да бъде индентифицирано. Най-общо те могат да бъдат разделени в следните групи:
4.1) данни относно физическата идентичност на лицата – имена и паспортни данни, ЕГН, номер на лична карта, дата и място на издаване, адрес, телефони, месторождение, и др.;
4.2) данни относно образованието на лицата – вид на образованието, допълнителна квалификация, степени и звания и др.;
4.3) данни относно трудовата дейност на лицата – професионална биография и др.;
4.4) данни относно семейната идентичност на лицата – семейно положение, родствени връзки и др.;
4.5) медицински данни – здравен статус и др.;
4.6) данни относно икономическата идентичност на лицата – имотно и финансово състояние на физическото лице, доходи от трудови и граждански правоотношения и др.
4.7) данни относно гражданско-правния статус на лицата, като свидетелство за съдимост и др.

В СУБ допустими за съхранение и обработка са следните лични данни:

- от група 4.1: имена и паспортни данни, адрес, телефони, месторождение, и др.;
- пълен обем от група 4.2.

Не са допустими за събиране, съхранение и обработка специални (чувствителни) лични данни – разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични и биометрични данни, сексуална ориентация. Допустимите за обработка и съхранение лични данни служат единствено за изпълнение на мисията на СУБ, както е публично оповестена в Устава на СУБ.

5. Съхраняваните в СУБ масиви от лични данни се предоставят или разкриват на публични органи като: Национална агенция за приходите, Национален огигурителен институт, Министерство на вътрешните работи, правоохранителни органи и др. органи, които имат законово основание да изискват такива данни.

6. Личните данни се съхраняват в СУБ за неопределен срок, регламентиран за отделните масиви на документооборота от специализираните за това органи и нормативни документи.

7. В СУБ се извършва управление на риска по отношение на защитата на личните данни чрез оценка на риска въз основа на естеството, обхвата, контекста и целите на обработването и на последиците за правата на физическите лица, за които се отнасят личните данни. При инцидент, свързан със заплаха от несанкциониран достъп или манипулиране на съхраняваните лични данни АДМИНИСТРАТОРЪТ е задължен не по-късно от 72 часа да уведоми надзорния орган с описание на нарушението и описание на риска от възможни последици.

8. С цел недопускането на неправомерен достъп, изменение или разпространение, случайно или незаконно унищожаване, случайна загуба и всички други незаконни форми на обработване на личните данни, ОБРАБОТВАЩИЯТ прилага необходимите и съотносими към дейността му технически и организационни мерки, които могат да бъдат (изброяването не е изчерпателно):

8.1. Въвеждане на специална процедура за дефиниране и даване на права на достъп до данни и ресурси, като за всеки служител се определя съответно ниво на достъп до информацията, съдържаща лични данни, въз основа на длъжностната му позиция и неговите служебни задължения.
8.2. Предотвратяване на неоторизиран достъп до базите данни чрез пароли за достъп и контрол на правата на потребителите. Възможност за контрол на достъпа чрез log report от ИТ администратора.
8.3. Физически достъп до сгради и помещения, в които се съхраняват регистри с лични данни, да се дава само на служителите, които са изрично оторизирани да обработват лични данни.
8.4. За по-доброто организиране на достъпа до работните помещения да се използват и способи като: а) съставяне списъци на оторизираните лица; б) въвеждане на специален режим за съхраняване на ключове от помещения, каси и други съоръжения, служещи за

съхраняване на информация, която съдържа лични данни; в) поддържане на антивирусни програми; д) наличие на архивираща система.

9. Обработващите лични данни се задължават да осигурят спазването на следните изисквания:
9.1. да използват личните данни, до които имат достъп, пропорционално на целите, за които са били предоставени от АДМИНИСТРАТОРА и да не ги обработват допълнително по начин, несъвместим с тези цели.
9.2. да не променят информацията относно предоставените лични данни от АДМИНИСТРАТОРА. Дори да се налага промяна (неверни данни, допълване), новите данни не заместват старите, а се добавят към тях.
9.3. да не разпространяват помежду си и/или да не предоставят на трети лица информация, съставляваща лични данни, станала им известна при или по повод изпълнение на служебни задължения, с изключение на случаите, когато разкриването й е предвидено със закон.
9.4. да бъде проведен инструктаж на ОБРАБОТВАЩИТЕ във връзка със задълженията им да обработват личните данни, до които имат достъп, законосъобразно, добросъвестно и само съобразно целите на сключения между ОБРАБОТВАЩИЯ и АДМИНИСТРАТОРА договор.
9.5. ОБРАБОТВАЩИЯТ да получава достъп до лични данни само след като е запознат с изискванията на законодателството, регулиращо защитата на лични данни, както и с настоящата инструкция.
9.6. Изискванията относно обработващия да бъдат спазвани и по отношение на всички останали лица, работещи за ОБРАБОТВАЩИЯ на основание, различно от трудов договор.

10. Физическите лица, за които в СУБ се събират, съхраняват и обработват лични данни имат право на достъп до собствените данни, на коригиране на данните, на изтриване на данните (т.н. „право да бъдеш забравен“), на ограничаване на обработването, на извършване на и контрол върху трансфера на личните данни, на възражение срещу автоматични решения, основани на профилиране (т.е. на решения, отнасящи се към определена група или категория служители). Те имат и право на жалба до надзорен орган (включително КЗЛД) при неспазване на посочените техни права от АДМИНИСТРАТОРА и/или ОБРАБОТВАЩИЯ.

11. ОБРАБОТВАЩИТЕ следва да съобразяват всички свои действия с изискванията на законодателството (Закон за защита на личните данни, Наредба №1 от 10.02.2010 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и др.), както и с установените най-добри международни практики при обработването на лични данни.