ЛИЧНИТЕ ДАННИ В КОНТЕКСТА НА ТРУДОВИТЕ ОТНОШЕНИЯ

гл. ас. д-р Паулина Иванова
Икономически университет – Варна

PERSONAL DATA IN THE CONTEXT OF EMPLOYMENT RELATIONS

Chief assist. Pavlina Ivanova, PhD
University of Economics – Varna, Bulgaria

Резюме: За целите на трудовото правоотношение по силата на законодателството работодателите събират, обработват и съхраняват определен обем лични данни на кандидатите за работа – работници и служители. Това поражда за тях съответни задължения и отговорности в качеството им на администратори на лични данни. В доклада са разгледани основанията за събиране и обработване на лични данни за целите на трудово правоотношение и са посочени необходимите мерки, гарантиращи поверителността на личните данни на персонала.

Ключови думи: *трудови отношения, лични данни, съгласие, работодател, работник*

Abstract: For the purposes of the employment relationship under the law, employers collect, process and store a certain amount of personal data of job candidates and employees. This creates for them respective obligations and responsibilities in their capacity as controllers of personal data. The report examines the grounds for the collection and processing of personal data for the purposes of employment and sets out the necessary measures to ensure the confidentiality of personal data of staff.

Key words: *employment relations, personal data, consent, employer, worker*

DOI: <https://doi.org/10.36997/PPDD2021.116>

Въведение

При предоставянето на работна сила отношенията между работодател и работник се уреждат като трудови правоотношения. Именно като вид обществено отношение трудовото правоотношение изразява връзката между хората по повод използването и въздействието на работната сила. Трудовото правоотношение „се характеризира със своя обект, страни, съдържание, както и с юридическите факти, основание за неговото възникване, изменение и прекратяване“ (Андреева, Йолова 2020). Основният нормативен акт, регламентиращ трудовите правоотношения в България, е Кодексът на труда (КТ), приет през 1986 г.

Трудовото правоотношение възниква при сключване на трудов договор, който регламентира съвкупността от права и задължения на страните, т.е. на работника или служителя и работодателя (Мръчков и др. 2009). Той има конкретно съдържание, включващо определени от закона данни за страните, определени в пар. 1, т. 10 от Допълнителните разпоредби на Кодекса на труда:

- за работодател – юридическо лице или едноличен търговец – наименование, седалище и адрес на управление на юридическото лице или едноличния търговец, ЕИК, имена на представляващия, единния граждански номер (личния номер – за чужденец); за работодател – физическо лице – името на лицето, постоянния адрес, единния граждански номер (личния номер – за чужденец);

- за работник или служител – името на лицето, постоянния адрес, единния граждански номер (личния номер – за чужденец), вида и степента на притежаваното образование, както и данни за притежаваната научна степен, ако е свързана с изпълняваната от него работа.

По своята същност този тип данни представляват лични данни. Такива работодателите събират, съхраняват и обработват още преди възникването на трудовото отношение, по време на неговото време-траене и след неговото прекратяване. В трудовото законодателство се съдържат относително ограничен брой разпоредби, определящи отговорността и границите на контрол на работодателя при администрирането, съхраняването и трансфера на лични данни на работещите. Нормативните актове, определящи изискванията към работодателите по отношение на събираните и съхранявани лични данни при и по повод на трудовите отношения, са Общият регламент относно

защита на личните данни (Регламент (ЕС) 2016/679), (ОРЗЛД) и Законът за защита на личните данни (ЗЗЛД).

Съгласно посочените актове лични данни са тези, които позволяват с тяхна помощ едно лице да бъде идентифицирано – лични данни могат да са името и фамилията, датата на раждане, адрес, номер на банкова сметка, информация относно образование и работен опит, телефонен номер, електронна поща, видео запис и т.н.

Националният надзорен орган по защита на личните данни е Комисията по защита на личните данни (КЗЛД). При изпълнение на своята контролна функция КЗЛД подпомага засегнатите лица, като събира служебно доказателства и възлага извършването на проверки (Матеева 2020).

В този контекст в настоящия доклад се разглеждат основанията за събиране и обработване лични данни за целите на трудово правоотношение, като се посочват и необходимите мерки, гарантиращи поверителността на личните данни на персонала.

Изложение

Работодателите, в качеството си на администратори на лични данни,¹ събират, обработват и съхраняват определен обем лични данни за целите на трудовото правоотношение по силата на Кодекса на труда, Кодекса за социалното осигуряване, Закона за счетоводството, както и други нормативни актове. Това определя законосъобразността на действията им, които в зависимост от хипотезата са законово задължение и/или са в съответствие с изпълнението на договор – „Обработването на лични данни от администратори както в публичната, така и в частната сфера е законосъобразно, ако е налице някое от следните алтернативни и равнопоставени основания: съгласие; изпълнение на договор; законово задължение; жизненоважни интереси; обществен интерес/официални правомощия; легитимни интереси“ (<https://www.cdpd.bg>).

¹ Администратор на лични данни – всяка организация, която определя целта и средствата за обработване на лични данни, извършва такова обработване и е отговорна за обработването или субект, който е задължен да извърши обработване на лични данни по закон.

Личните данни в процеса по набор и подбор на персонал

Събирането и обработването на лични данни от страна работодателите започва още в процеса по набиране и подбор на персонал. Кандидатите за работа, независимо от начина, по който адресират своята кандидатура, сами разкриват лични данни пред различните компании или институции. Представяните от тях данни са в съдържание и обем, определени от работодателя при обявяване на свободната работна позиция или обявяването на конкурс за съответната длъжност. Изхождайки от разпоредбите на ЗЗЛД и ОРЗЛД, потенциалният работодател следва да изисква само такива данни, които са съотнесими към процеса на подбор, т.е. те да са важни и съществени по отношение вземането на решение за наемане на дадения кандидат.

Обичайно кандидатстването за работа изисква представянето на автобиография, съдържаща идентификационни данни (име, фамилия, дата на раждане), данни за контакт (адрес по местоживее, телефонен номер, електронна поща), както и информация за образование, умения, професионален опит. Кандидатите сами решават каква точно информация да разкрият в автобиографията си, включително и дали да предоставят снимка (изискване за предоставяне на снимка не е изрично регламентирано в нормативен акт). В рамките на етапа по кандидатстване за дадена позиция няма и основание да се изисква банкова информация, както и копие от документ за самоличност.

Понякога компаниите включват към набора от документи за кандидатстване съгласие² за обработване на личните данни за целите на подбора. Това е възможно, но не е изрично необходимо, когато се кандидатства по конкретна обява и данните се предоставят директно на потенциалния работодател (Защита на неприкосновеността на работното място. Наръчник за служители, (<https://www.cdpd.bg/>)). Кога обаче това все пак е необходимо? Наличието на съгласие от страна на кандидатите за работа е необходимо, когато работодателят предложи и кандидатът приеме автобиографията и останалият набор от документи да бъдат използвани при бъдещ подбор на персонал. Някои организации на базата на даденото съгласие включват личните данни на кандидатите, които не са назначени в своята база данни от потен-

² Съгласие – свободно, конкретно и информирано изразяване на волята на субекта на данни, което съдържа разрешение за обработване на лични данни, които се отнасят до него.

циални работници.

Част от процеса по подбор може да включва и провеждането на интервю. По време на интервюто работодателят, с цел да изясни конкретни обстоятелства от автобиографията на кандидата за работа, може да задава въпроси, които са свързани само със съответната работна позиция. Лицата имат право да не отговарят на въпроси, които ги смущават – например, отнасящи се до религиозни убеждения, политически възгледи, частен живот, семеен статус, сексуална ориентация, планове за създаване на семейство. Когато обаче има законово основание за това, работодателят има право да задава въпроси, касаещи чувствителни данни – например за съдебното минало на лицето, ако това е съотносимо към длъжността, или за здравословно състояние, ако има медицинска забрана за заемане на длъжността от лица с определени заболявания или конкретно състояние.

Работодателите биха могли да се сдобият и с допълнителна информация за търсещите работа от социалните мрежи, постовете им в интернет форуми, и това да повлияе решението им за наемане. Какво обаче е видно за лицата в интернет пространството и профилите им в социалните мрежи е тяхно лично решение. Ако те са позволили споделянето от тях информация, снимки и преживявания да са публични, това създава предпоставка те да бъдат използвани за различни цели, т.е. онлайн неприкосновеността е отговорност на самите лица.

С промените в Закона за защита на личните данни от 2019 г. се регламентира срокът за съхранение на данните на кандидатите за работа. Разпоредбата е работодателят или органът по назначаването, в качеството си на администратор на лични данни, да определи срок за съхранение на личните данни. Този срок не може да е по-дълъг от 6 месеца, освен ако кандидатът не е дал съгласието си за съхранение за по-дълъг срок. След изтичането му работодателят трябва да изтрие или унищожи съхраняваните документи с лични данни, освен ако специален закон не предвижда друго. Той няма право да използва данните, съдържащи се в автобиографиите на лицата, за други цели. Друго изискване е, когато работодателят е поискал да се представят оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, той да върне тези документи на кандидата, който не е одобрен за назначава-

не, в 6-месечен срок от окончателното приключване на процедурата, освен ако специален закон не предвижда друго.

Личните данни при назначаване и по време на трудовото правоотношение и след неговото прекратяване

С избраните в процеса на подбор кандидати се сключва трудов договор, което от своя страна инициира създаването на личното трудово досие. То съдържа документите, необходими за сключването на трудовия договор, една част от които са предоставени от лицата и други, подготвени от работодателя. Документите могат да бъдат класифицирани като задължителни – изискващи се съгласно Кодекса на труда и Наредба № 4 за документите, които са необходими за сключване на трудов договор и допълнителни. Повечето от тях съдържат лични данни за работещия, а някои от тях – и данни за трети лица (деца, съпруг, съпруга). Когато в рамките на трудовото правоотношение се налага събирането и обработването на специални категории (чувствителни) лични данни – религиозни убеждения, синдикално членство, биометрични данни, данни за здравословното състояние, сексуална ориентация и др., се съблюдават разпоредбите на чл. 9, пар. 2 от ОРЗЛД. Независимо че говорим за трудово досие, в него може да се съдържат освен данни за трудовото правоотношение и данни от личния живот на работника или служителя. Те се предоставят лично от него при настъпване на определени обстоятелства в неговия личен живот. Целта е работникът да се възползва от своите права, а работодателят – да изпълни своите административни задължения. Пример в това отношение са отпуските за бременност и раждане, за отглеждане на дете и отпуските за изпълнение на граждански, обществени и други задължения (встъпване в брак, кръводаряване, смърт на близък роднина).

В контекста на трудовите правоотношения работодателят е длъжен да не разкрива личните данни на работника или служителя на трети лица. Достъп до личните данни на персонала могат да имат служителите, които изрично са упълномощени да ги обработват. Те могат да бъдат разкривани на външни субекти, само когато за това има нормативно основание – например при проверка от Инспекцията по труда. Данните се предоставят и пред компетентните органи във връзка със социалното и здравно осигуряване, както и във всеки друг случай, предвиден в националното законодателство (чл. 6, (41), (45)

от Регламент (ЕС) 2016/679).

Тъй като основен принцип при защита на личните данни е те да бъдат съхранявани докато това е необходимо, важно за работодателите е да определят тези срокове според нормативните изисквания и спецификата на своята дейност. Една част от трудовото досие на работника, касаеща трудов и осигурителен стаж, следва да се съхранява за периода на съхранение на разчетно-платежните ведомости (50 години), друга част от документите е достатъчно да бъдат съхранявани до изтичане на определения в Кодекса на труда давностен срок за предявяване на искове по трудови спорове.

Личните данни на персонала могат да бъдат обработвани и след прекратяване на трудовото правоотношение. Правните основания за това са значително по-малко, обикновено са във връзка с целите на пенсионното и здравното осигуряване, данъчни и архивни цели, както и в случаите на възникнал трудов спор пред съда.

Мерки, гарантиращи поверителността на личните данни на работещите

Тъй като националното трудово законодателство не съдържа специфични разпоредби, необходимо е процесът по защита на данните и свързаният с това контрол да бъдат организирани от всеки работодател чрез разработване на вътрешни документи (Матеева 2018). Те трябва да отговарят на изискванията и принципите на ОРЗЛД и произтичащите от него конкретни задължения за администраторите на лични данни и в частност на работодателите. Обобщени конкретните мерки, които работодателите следва да предприемат са представени в таблица 1.

Таблица 1

Мерки, гарантиращи поверителността на личните данни на персонала

Изграждане на ясна система за обработка на личните данни
Създаване на вътрешни за организацията нормативни документи, които да регламентират обработката и съхранението на данните
Периодично ревизиране на въведената система
Използване на надеждни технологии с подходящи нива на защита на личните данни

Осигуряване на адекватни технически и организационни мерки за защита на личните данни, обработвани в рамките на трудовото правоотношение
Разработване на прозрачни фирмени политики за защита на личните данни
Ясна информация за събирането на лични данни
Уточняване на целите за обработка на лични данни
Дефиниране на правилата за запазване и изтриване на лични данни
Използване на подходяща защита за съхранението на личните данни
Уведомяване на властите за нарушения във връзка с лични данни
Получаване на подходящо съгласие за обработка на данни
Съхраняване на записи с подробна обработка на данните
Обучения на служители, които обработват лични данни
Одит и актуализиране на политиките за лични данни
Назначаване на DPO – Длъжностно лице по личните данни ³ (ако е необходимо)

В конкретика подходящите технически и организационни мерки за осигуряване на сигурност на данните се изразяват във:

- псевдонимизация на данните;
- криптиране на данните;
- осигуряване на постоянна поверителност на системите за обработване;
- в случай на физически или технически инцидент – своевременно възстановяване на наличността и достъпа до личните данните;
- провеждане на редовни изпитания на техническите и организационните мерки;
- сътрудничество с надзорния орган за защита на личните данни.

³ Длъжностно лице по личните данни – служител на администратор на лични данни или външно за организацията на администратора физическо лице, натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията на администратора и повишаването на осведомеността и обучението на персонала.

Заклучение

В контекста на изложеното може да се обобщи, че:

- Събирането, обработването и съхранението на лични данни за целите на трудовото правоотношение е в съответствие със законово задължение на работодателите или е във връзка с изпълнението колективния и/или индивидуалния трудов договор.

- Изрично съгласие от страна на кандидатите за работа, работниците и служителите се изисква само при определени обстоятелства.

- Субектът на данните (физическото лице, за което се отнасят данните) има право на информираност, достъп до собствените си лични данни, коригиране (ако данните са неточни), право на защита по съдебен или административен ред, в случай че правата му по отношение на личните данни са били нарушени.

- Работодателят може да съхранява лични данни на персонала за период, определен от съответните нормативни актове. След изтичане на този срок, данните следва да бъдат унищожени. Това поражда правото на кандидатите за работа и работещите „да бъдат забравени“.

- Техническите и организационни мерки за защита на данните, които работодателите прилагат трябва да са адекватни на рисковете и на категориите данни.

Основният инструмент за доказване и удостоверяване на законсъобразното, добросъвестно, прозрачно и с подходящо ниво на сигурност и защита обработване на лични данни е отчетността, която е въведена като задължение на администраторите с ОРЗЛД. В Република България контролът по спазването на изискванията във връзка със защитата на личните данни се осъществява от Комисията за защита на личните данни, която има право да се произнася по жалби на физически лица, да проверява администратори и обработващи лични данни, да издава становища, задължителни предписания и да налага санкции.

Използвана литература

Андреева, А. Г. Йолова (2020). Трудово и осигурително право. Варна: Наука и икономика.

Защита на неприкосновеността на работното място. Наръчник

за служители, (<https://www.cdpd.bg>, 30.09.2020).

Мръчков, В., К. Средкова, А. Василев (2009). Коментар на кодекса на труда. София: Сибм.

Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679), (<https://www.cdpd.bg>, 30.09.2020).

Andreeva, A., Z. Mateeva (2018). Employers as Personal Data Administrators – Specifics and Requirements in the Context of the Information Society. Globalization, the State and the Individual. Varna: VFU Chernorizets Hrabar.

Mateeva, Z. (2020). Protection of Persons of Personal Data Before the National Supervisory Authority. Burgas: Miracle A Ltd.

За контакти: гл.ас. д-р Павлина Иванова
Икономически университет – Варна
e-mail: p.ivanova@ue-varna.bg