ЛИЧНИ ДАННИ
кога и защо можем (не можем) да обработваме лични данни

www.NFTINI.org

Лични данни е всяка единица информация, от която може да се направи пряк или косвен извод за самоличността на някого или за негова индивидуална или групова характеристика.

> Пример за лични данни са конкретни **идентификатори, които обозначават еднозначно лицето**: име, ЕГН, снимка на лицето, пръстов отпечатък, ДНК. Пример за лични данни са и такива идентификатори, които не обозначават никого еднозначно, но **разкриват определена харакеристика на лицето**: пол, адрес, телефон, месторабота, образование, финансово състояние, влечение, политически възглед, религиозно вярване, заболяване, увреждане. Пример за лични данни са и такива идентификатори, които обикновено изобщо не свързват с понятието „данни“, но **в даден контекст могат да бъдат ползвани** като идентификатор: цвят на служебния бадж, папка с логото синдикална организация, източно-европейски акцент при ползването на чужд език. С други думи – при определени обстоятелства почти всяка информация може да се разглежда като „лични данни“.

Обработване на лични данни е всяка дейност, насочена към придобиване, записване, съхраняване, преглеждане, систематизиране, изтриване, заличаване (не е същото като изтриване) и предаване на данни към трета страна.

> Пример за обработване на лични данни е приемането на Заявления за синдикално членство, попълването на Списък с присъствалите лица на синдикално събрание, съхраняването на учредителни протоколи на синдикални секции, предоставянето на Работодателя на списък с работещи при него синдикалисти за удържане на членския внос по ведомост, изготвянето на файл с адреси и телефони на синдикални експерти, фотографирането на стачкуващ синдикалист със знаме на КТ „Подкрепа“, записването на такъв синдикалист от охранителните камери в предприятието, записването на данни за телефонно повикване до стачкуващ колега, записването на данни за посещаване на www.Podkrepa.net от служебния компютър и други подобни.

При обработването на лични данни следва да се обезпечи **ниво на информационна сигурност**, което е толкова по-високо, колкото по-голям е рискът за лицата, чиито данни се обработват.

> Рискът се определя от **броя лица**, за които данните се отнасят (колкото повече лица, толкова по-голям риск); от **естеството на данните** (колкото по-интимни и изобличаващи данни, толкова по-голям риск); от **повода за обработване** на данните (колкото по-индиректно са получени данните и за това не е получено съгласие от лицата, толкова по-голям риск); от **начина на обработване** на данните (колкото по-задълбочен анализ и проникване в лицната сфера на лицата се осъществява, толкова по-голям риск).

Регламент (**ЕС**) **2016/679** от **27.04.2016** г. за защита на физическите лица във връзка с обработването на лични данни и за свободното движение на такива данни (**GDPR**) е най-мащабната **нормативна уредба на данните**, извършена централизирано за Европейскския съюз с цел обработването на лични данни да бъде подчинено на **единни стандарти** и адекватни нива на **информационна сигурност**. Регламентът няма за цел да забрани обработването на данни, нито има за цел да наложи огромни парични санкции (както често се спекулира) – а е насочен към въвеждането на правила, които да гарантират обработването на лични данни само тогава и само дотолкова, когато и доколкото това е **наистина необходимо**.

В много от случаите създадената **истерия** около **Регламент** (**ЕС**) **2016/679** (повсеместно попълване на „декларации за съгласие“ в бензиностанции, аптеки, магазини; натрапване на скъпо струващи обучения, без които „със сигурност ще бъде наложена огромна санкция“; въвеждане на всякакви правила за защита на данните, правила за поверителност, правила за конфиденциалност...) е **напълно излишна**. Въпреки, че Регламентът е доста сложно и объркано написан, и предвижда значителни санкции, в крайна сметка **систематизира отдавна съществуващи концепции** и въвежда необходимата систематизация в контекста на съвременните информационни и комуникационни технологии.

Основните принципи, чието спазване би удовлетворило повечето изисквания за защита на данните, могат да се обобщят така:

- данните трябва да бъдат сведени до **минимум** (колкото по-малко данни, толкова по-добре);
- трябва да се обработват само данни, които са наистина **необходими** (не „за всеки случай“);
- на всяко обработване на данни трябва да съответства **легитимна** законова цел („защо-затова“);
- всяко обработване трябва да е ясно **обозначено** и известно на лицата, за които се отнася;
- лицата, за които данните се отнасят, **могат** да преглеждат и поправят данните и да ги блокират;
- данните трябва да се унищожават (заличават) **веднага**, след като вече не са необходими;
- колкото повече данни, за повече лица и по-чувствителни данни, толкова повече **сигурност**;
- **предаване** на данни към трети страни само доколкото това има легитимна цел и е сигурно.

Синдикалните организации заемат привилегировано положение при обработване на данни на свои членове и при обработване на данни във връзка с изпълнението на техни синдикални функции.

Чл. **6**, **§1**, б.б. „**а**“ и „**б**“ от **Регламент** (**ЕС**) **2016/679** определят като **законосъобразно** обработване на лични данни, за което *„**субектът на данните е дал съгласие*** (...) *за една или повече конкретни цели“* или което е *„необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор“*. С попълването на **Заявление за членство** лицата **дават съгласие** личните им данни да бъдат обработени за **конкретна легитимна цел** – да бъдат третирани като синдикални членове. Въпреки, че повечето хора не биха разглеждали **синдикалното членство като договор**, от юридическа страна то е именно такова – нито синдикалният член може да изпълни задълженията си към своята синдикална организация без обработването на лични данни, нито синдикалната организация може да изпълни своите задължения към него без такова обработване.

Децентрализираният характер на синдикалните организации издига защитата на личните данни на техни членове на много високо ниво, без самите организации да е необходимо да полагат някакви специални усилия: **данните просто ги няма в единен централизиран регистър**, който би могъл да стане предмет на значителни нарушения, обхващащи голям брой лица или техни чувствителни данни. **Професионалните организации** и **Регионалните организации** съхраняват единствено данни за броя синдикални членове, но не и техните лични данни. **Синдикалните секции** съхраняват лични данни на своите членове, но те са по-малки по обем и възможностите за злоупотреба с наличната при тях документация е ограничена.

Независимо от горните предпоставки за сигурност на информацията при синдикалните организации, е полезно да спазваш някои **технически и организационни мерки за информационна сигурност**.

> **Не дръж синдикална документация** (и особено списъци със синдикални членове и заявления за членство) в помещението, предоставено на вашата синдикална секция от Работодателя по силата на

неговите задължения – поне не до момента, в който не сключите Колективен трудов договор и отношенията ви придобият цивилизован вид.

Не се свързвай със синдикални дейци **по телефони или от компютри, предоставени от Работодателя** или под негов или на негови партньори контрол – особено когато отношенията са изострени, например поради подготовката и провеждането на **ефективна стачка**.

Дръж синдикалната документация на хартия под ключ (не е необходима огнеупорна каса, достатъчно е чекмеджето на бюрото ти у дома), а документацията **в електронен вид – в компютър, защитен с парола и по възможност шифрована**; и обновявай редовно софтуера на компютъра.

Не провеждай синдикални срещи на места, които са **в полезрението на Работодателя** или на негови партньори – особено когато отношенията са изострени, например поради назряващо недоволство в предприятието, довело до учредяване на синдикалната секция, за която още не се знае официално в предприятието.

Не дискутирай с трети страни **източниците и естеството на поверителна информация** – независимо дали са синдикални членове или други колеги от предприятието – освен в рамките на необходимото за защита на правата и с **минимум** (**по възможност никакви**) **лични данни**.

Запознавай останалите синдикални членове със значението на информационната сигурност и ги приучвай към това да пазят като служебна тайна всичко, което се случва в синдикалната секция и което се споделя между синдикелните дейци.

Чл. **6**, **§1**, б.б. „**в**“ и „**г**“ от **Регламент** (**ЕС**) **2016/679** определят като **законосъобразно** обработване на лични данни, *„**необходимо за спазването на законово задължение**, което се прилага спрямо администратора“* или което е *„необходимо, за да бъдат защитени жизнено-важните интереси на субекта на данните или на друго физическо лице“*. Съгласно чл. **406**, ал. **2**, т.т. **1-3** във вр. с ал. **1** от **Кодекса на труда**, *„синдикалните организации имат право да сигнализират контролните органи за нарушения на трудовото законодателство“*, във връзка с което *„представителите на синдикалните организации имат право: **1.** да посещават по всяко време предприятията и другите места, където се извършва работата, както и помещения, ползвани от работниците и служителите; **2.** да изискват от Работодателя обяснения и представяне на необходимите им сведения и документи; **3.** да се осведомяват пряко от работниците и служителите по всички въпроси по спазване на трудовото законодателство“*. С упражняването на горните **законови правомощия**, синдикалните организации освен всичко друго **защитават жизнено важен интерес** – интереса на работещите хора да бъде упражняван контрол за безопасност и здраве при работа и за спазване на трудовите им права.

Често Работодатели злоупотребяват с **Регламент** (**ЕС**) **2016/679**, като отказват достъп на синдикалните дейци до определени данни, под предлог, че това било „защита на лични данни“. В такава ситуация можеш да противопоставиш чл. **403**, ал. **1**, т.т. **1** и **2** във вр. с чл. **406**, ал. **3** от **Кодекса на труда**, съгласно които *„представителите на синдикалните организации при изпълняване на сигналната си функция са длъжни“* (...) *„**1.** да пазят в тайна поверителните и за служебно ползуване сведения, които са им станали известни във връзка с упражняването на контрола, както и да не използуват тези сведения в своя стопанска дейност; **2.** да пазят в тайна източника, от който са получили сигнал за нарушение на трудовото законодателство или на законодателството, свързано с държавната служба“*.

Синдикалните дейци при изпълнение на техните функции се приравняват на **контролни органи**. Първо, във връзка със своите законови правомощия те **имат право на достъп до всяка информация**, свързана със спазване на трудовото законодателство. И второ – те нямат право да разкриват и от тях

не може да се иска **никаква информация** за техни синдикални членове и за подадени от тях сигнали и сведения за нарушаване на трудовото законодателство. Единствено изключение в тази връзка е задължението на синдикалната организация след сключването на **Колективен трудов договор** да представи на Работодателя списък на своите членове, на които да бъдат признати договорените социални придобивки. Синдикалните дейци нямат право да разкриват и никакви поверителни сведения за Работодателя, освен в предвидените от закона случаи – например пред **контролните органи** по инспектиране на труда или пред **съдебните органи**.

Често срещана злоупотреба от страна на някои Работодатели е внушаването на работещите при тях, че **разкриването на каквато и да било информация** от тяхна страна, пред когото и да било и при какъвто и да било повод, ще бъде санкционирана с глоби, неустойки, дисциплинарно преследване. Първо, **уговарянето на „глоби“ и „неустойки“ е недействително**. В българското трудово право са допустими само три дисциплинарни наказания: забележка, предупреждение и уволнение. И второ – с подобни действия Работодателят **не може да препятства съобщаването на нарушения** пред синдикалните организации, пред контролните органи и пред Съда. Никой не може да бъде преследван заради това, че е разкрил нарушение на закона или е предприел действия за отстраняване на нарушението и за санкциониране на виновниците.

Каквото и да разкриеш пред синдикалните дейци, то е служебна тайна по силата на цитираните по-горе норми на чл. **403**, ал. **1**, т.т. **1** и **2** във вр. с чл. **406**, ал. **3** от **Кодекса на труда**. Ако ползваш съдействието на адвокат (било в синдикалната организация, било другаде), всичко казано помежду ви е **адвокатска тайна** – то не може да бъде узнавано, записвано и използвано от трети лица по никакъв повод. Дори да представлява доказателство за извършени престъпления и да включва направени самопризнания, то не може да бъде приложено като доказателство (освен като доказателство за това, че този, който го разкрива, е нарушил адвокатската тайна и подлежи на санкция за това).