ИЗСЛЕДВАНЕ НА ВЪЗДЕЙСТВИЕТО

КАЗУС 1 - ФРАНЦИЯ

GDPR: въздействие върху компаниите

Предговор

Общият регламент за защита на данните 2016/679 от 27 април 2016 г. (GDPR), влязъл в сила на 25 май 2018 г., заменя системата от предходни формалности, предвидена в Закона за защита на данните, система, основана на отговорността на участниците, които ще трябва да демонстрират съответствието на своите обработки с този регламент по всяко време.

1) Специфичността на регламента: пряко и незабавно прилагане от 25 май 2018 г. във всички страни на ЕС, без да се изисква, противно на директивата, транспониране в различните държави-членки. Правилниците, вече приложени към тази дата, трябва да бъдат приведени в съответствие с нейните разпоредби.

Националната комисия по защита на личните данни, подкрепа на иновациите и запазване на индивидуалните права и свободи (CNIL) на своя уебсайт и в няколко практически ръководства анализира въздействието на влизането в сила на този текст, особено за компаниите. Следователно нашият казус ще възобнови съдържанието на указанията, дадени от CNIL относно отношенията между служителите и тяхната компания.

Забележка:

GDPR се прилага за много области и не предвижда конкретни правила за трудовото законодателство, оставяйки го на държавите-членки да определят в този случай адаптациите, които считат за необходими. Проектозаконът за личните данни, окончателно приет от Парламента на 14 май 2018 г. и за изменение на Закона за защита на данните (Закон 78-17 от 6 януари 1978 г.), съдържа само няколко разпоредби, специфични за трудовите правоотношения, с изключение на обработката на определени данни.

Нашият казус има за цел да представи промените, въведени от GDPR в сравнение с предходното законодателство.

2) Преходът от понятието за предходни формалности (декларация, разрешения), съдържащо се в старата директива 95/46 / CE от 24 октомври 1995 г., към логиката за съответствие, за която участниците са отговорни, под контрола на CNIL чрез Новия Европейски Регламент.

Обработващите лични данни трябва да прилагат всички технически и организационни мерки, необходими за отчитане на защитата на личните данни, от дизайна на продукта или услугата, тоест да могат да докажат спазването на техните обработки по всяко време.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Последицата от това овластяване на участниците е премахването на предходните декларационни задължения.

Всъщност, преди въвеждането на разпоредбите на GDPR в компанията, CSE трябваше да бъде информиран за процесите на автоматизирано управление на персонала и всички промени в тях (член L 2312-38 от Кодекса на труда). Това премахване на изискванията за отчитане вероятно ще създаде трудности в случай на съдебни спорове. Липсата на задължителна декларация до CNIL позволи на санкциониран или уволнен служител да разчита на недопустимостта на доказателствата за предполагаемите факти, получени от недекларирано устройство за контрол. Това вече не е така.

3) Разпоредбите, за които се отнася GDPR: всяка организация, независимо от нейния размер, страна на регистрация и дейност, може да бъде засегната.

Всъщност GDPR се прилага за всяка организация (публична или частна), независимо от нейния размер, страна на дейност или дейност, в случай, че обработва лични данни от нейно име или не, и когато:

• е създадена на територията на Европейския съюз;

• дейността ѝ е насочена пряко към европейските жители.

Пример: Компания, създадена във Франция, изнасяща всичките си продукти извън Европейския съюз, трябва да спазва GDPR.

RGPD също е насочена към подизпълнителите, които управляват лични данни от името на други организации (например компании).

Подизпълнителите са обект на специфични задължения: защита на личните данни и неприкосновеността на личния живот от дизайна на тяхната услуга или продукт, съвети на техните клиенти, водене на отчет за дейностите по обработка, извършвани за сметка на техните клиенти. Договорът за подизпълнител трябва да включва специфична клауза за защита на личните данни.

4) Съответните данни са така наречените лични данни, т.е. всяка информация, позволяваща пряко идентифициране (фамилия, име, например) или косвено (номер на клиент, телефонен номер, номер на регистрация за управление на паркинг, биометрични данни и т.н. .) на човек.

Човек може да бъде идентифициран чрез своето ЕГН (напр. Социалноосигурителен номер) или чрез компллекс от набор от данни (лице, живеещо на такъв адрес, родено в този ден, абонат на такова списание и активист в такова сдружение).

Забележка:

IP и Mac адресите са лични данни (Cass, 1st civ 3-11-2016 No. 15-22.595 FS-PB).

Събирането на определени данни трябва да породи особена бдителност, особено тези, свързани с възползване от правата на служителите, доколкото те могат да представляват информация за тяхната сексуална ориентация.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Понятието досие обхваща всеки структуриран набор от лични данни, достъпен според определени критерии, независимо дали този набор е централизиран, децентрализиран или разпределен функционално или географски (напр. досиета, подредени по азбучен ред или хронологично).

Обработката на лични данни е операция или набор от операции, свързани с лични данни, независимо от използвания процес (събиране, записване, организация, запазване, адаптиране, модификация, извличане, консултации, използване, комуникация чрез предаване, разпространение или друга форма на осигуряване, помирение).

Забележка:

Досие, съдържащо само информация за връзка с фирмата (например фирма „Фирма А“ с пощенския си адрес, телефонния номер на нейния офис и общ имейл за контакт „compagnieA@email.fr“) не е обработка на лични данни.

Освен това обработката на лични данни не е непременно компютърна: хартиените досиета също са засегнати и трябва също да бъдат защитени.

Обработката на лични данни трябва да има цел. Не е възможно да се събират или обработват лични данни само в случай, че някой ден могат да се окажат полезни.

5) Хората, засегнати от GDPR

• Администраторът е физическото или юридическото лице, публичният орган, службата или друг орган, който сам или съвместно с други лица определя целите и средствата на обработването и относно задълженията, предвидени в наредбата.

• Лицето, за което се отнася обработвването на лични данни, е лицето, с което е свързан субекта на личните данни.

• Администраторът е всяко физическо или юридическо лице, публичен орган, служба или друг орган, който получава лични данни, независимо дали е от трета страна, или не от трето лице, последният “от всяко лице, различно от субекта на данните, администратора, обработващият и лица, които под прякото ръководство на администратора или обработващия са упълномощени да обработват лични данни.

6) Принципите, въведени от GDPR

Регламентът се основава на принципите, според които личните данни трябва да:

• се третират по законен, справедлив и прозрачен начин по отношение на съответното лице;

• са събрани за конкретни, изрични и законни цели и не се обработват по начин, несъвместим с тези цели;

• са адекватни, уместни и ограничени до необходимото с оглед целите, за които се обработват (минимизиране на данните);

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

• са точни и актуални;

• се съхраняват във форма, позволяваща идентифициране на засегнатите лица за период, който не надвишава необходимия за целите, за които се обработват;

• се обработват, за да се осигури подходяща сигурност на личните данни, включително защита срещу неразрешено или незаконно обработване и загуба, унищожаване или случайно увреждане (неприкосновеност и конфиденциалност).

Забележка:

Конкретните действия, които трябва да бъдат изпълнени, за да се спазват принципите, установени от GDPR:

• назначаване на ръководител;

• регистриране на досиетата;

• идентифициране на рисковите елементи;

• зачитане правата на хората;

• защита на личните данни;

• гарантиране, в случай на възлагане на подизпълнители, че доставчикът на услуги ще спазва GDPR;

• назначаване на служител по защита на данните.

7) Служителят по защита на данните (DPO) е задължителен за публични органи и компании, чиято основна дейност води до редовен и систематичен мониторинг на големи групи или мащабна обработка на данни, наречени чувствителни или свързани с наказателни присъди и престъпления.

Въпреки това, дори ако компанията не е официално задължена да определи DPO, CNIL препоръчва назначаване на лице с добри вътреши взаимоотношения, за да се гарантира спазването на европейския регламент. Този човек е отговорен за спазването на изискванията за защита на данните в своята организация и е отговорен основно за:

• информиране и консултиране на администратора или подизпълнителя и техните служители;

• проследяване спазването на регламента и националния закон за защита на данните;

• съветване на компанията за извършване на проучвания за въздействие върху защитата на данните и мониторинг на тяхното прилагане;

• сътрудничество и представляване на звена за контакт на надзорния орган.

DPO може да бъде приложена вътрешно сред служителите на компанията или външно. Той може също да бъде споделен между няколко организации или в рамките на професионални асоциации или федерации.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Забележка:

Концепцията за широкомащабно прилагане не е дефинирана от RGPD, поради което CNIL даде илюстрации към тази концепция за "мащабно приложение": системи, управляващи данните на пътници, използващи обществен транспорт, или тези, свързани с техните клиенти, администрирани от банки, застрахователни компании, телефонни оператори или доставчици на интернет услуги.

8) Преброяването на данните налага задължението за водене на регистър на обработването на лични данни.

Въпреки, че това се отнася само за компании с най-малко 250 служители, CNIL препоръчва по-широкото му прилагане.

Целта е да се идентифицират основните дейности на компанията, които изискват събиране и обработка на данни (примери по отношение на управлението на човешките ресурси: набиране на персонал, управление на заплатите, обучение, социални декларации, задължителни, значки и управление на достъпа и др.).

За всяка дейност е необходимо да се изброят:

• администраторът;

• преследваната цел;

• категориите на използваните данни (напр. Ведомост: фамилия, име, дата на раждане, заплата и т.н.);

• хората с достъп до данните (получателят - пример: отдел за набиране на персонал, IT отдел, управление, доставчици, партньори, домакини);

• срокът на годност на тези данни (продължителността от време, през която данните са полезни от оперативна гледна точка и периода на съхраняване на архива).

Регистърът е под отговорността на управителя на дружеството.

Според CNIL не е необходимо в този регистър да се изброяват чисто случайни обработки, като например файлове, създадени за конкретна операция на събитие, като например откриването на магазин.

9) Целта, зададена на администратора, е да може по всяко време да докаже, че обработките, които той управлява, отговарят на правилата.

Следователно е важно да може да се определи релевантността на събраните данни чрез проверка на различни точки:

• обстоятелства за събиране на данни: имало ли е съгласие от субектите на данни? Ако не, събирането отговаря ли на конкретни задължения (събиране, изисквано за договора, спазване на законово задължение, например обработка на данни, свързани със служителите, които да комуникират със социалната сигурност или данъчната администрация ...);

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

• естеството на информацията, предоставяна на лицата, които се събират и третират: информирани ли са за целта на лечението и техните права?;

• естеството на данните, събрани по отношение на целта на лечението: могат да се събират и обработват само строго необходими за лечението данни;

• Информация, че само упълномощени лица имат достъп до необходимите им данни и че данните не се запазват извън необходимото.

10) Специфични случаи на обработка на данни, включващи повишена бдителност

Това се отнася за лечения, чиято цел или ефект е:

• Оценката на личните аспекти или на представата за човек;

• Автоматизирано вземане на решения;

• Систематичен мониторинг на хората: телемониторинг, мониторинг на социалните мрежи на служителите, анализ на страниците в социалните мрежи на кандидатите за работа, инструменти за управление на посещаемостта (напр. Бадж), геолокационни системи;

• Обработка на чувствителни данни. Чувствителни са данните, разкриващи предполагаемо расов или етнически произход, свързани с политически мнения, философски или религиозни, свързани с членството в профсъюзи, здравна или сексуална ориентация, генетични или биометрични данни, данни за престъпления или наказателна присъда;

• Обработка на данни относно уязвимите лица (например: непълнолетни лица);

• Иновативни приложения или прилагане на нови технологии (пример: свързан обект);

• Изключване на ползата от право, услуга или договор.

Когато обработката на данни отговаря на поне 2 от тези 9 критерия, трябва да се извърши оценка на въздействието върху поверителността (PIA). CNIL създаде софтуер, улесняващ провеждането и формализирането на анализа на въздействието: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil .

Забележка:

Член 8 от законопроекта за защита на личните данни, приет от Парламента на 14 май 2018 г., забранява обработката на чувствителни данни. Доколкото целта на обработването я изисква за определени категории данни, тази обработка няма да бъде предмет на тази забрана, по-специално обработването съгласно стандартните наредби, установени от CNIL, прилагани от работодателите и отнасящи се до строго биометрични данни. необходими за контрол на достъпа до работните места, както и до устройства и приложения, използвани в контекста на задачите, възложени на служители, обучаващи се или доставчици на услуги.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

В интерес на яснотата и подкрепата CNIL няма да изисква незабавно приключване на оценка на въздействието на съществуващите обработки, които редовно са били предмет на предварителна формалност с CNIL преди 25 май 2018 г. (даване на съгласие, декларация за съответствие с определени стандарти, разрешение, становище на CNIL) или които са записани в регистъра на компютъра и кореспондента на свободата. Засегнатите компании имат период от 3 години от 25 май 2018 г. за извършване на това проучване на въздействието. Този толеранс не се прилага за обработки на данни, възникнали преди 25 май 2018 г., той се прилагаше и преди това, но претърпя съществена промяна след приключването на официалното ѝ влизане в действие.

11) Специалният случай на трансфер на данни извън ЕС

В този случай ще бъде необходимо да се провери дали държавата, в която се прехвърлят данните, има законодателство за защита на личните данни и дали е признато надлежно от Европейската комисия.

Това е достъпно в CNIL.

Компанията ще трябва да контролира законността на своите трансфери, за да осигури защита на данните в чужбина.

12) Информация за служителите

Декларацията за събиране на данни, независимо от неговия характер (форма, въпросник и т.н.), трябва да включва изброената по-долу информация:

• идентичността и данните за контакт на администратора и, когато е подходящо, на представителя на администратора;

• когато е приложимо, данните за контакт на служителя по защита на данните;

• целите на обработването, за които са предназначени личните данни, и правното основание на обработването;

• съответните категории лични данни;

• когато е подходящо, получателите или категориите получатели на личните данни (вътрешна услуга на компанията, доставчик на услуги и т.н.);

• срок на годност на данните;

• условията, при които заинтересованите лица могат да упражняват правата си (чрез личното си пространство на уебсайта на компанията, чрез съобщение на специален имейл адрес, чрез пощенска услуга и т.н.);

• в случай на трансфер на данни извън Европейския съюз, посочване на съответната държава, наличието или липсата на документ засъответствие, издаден от Европейската комисия, или позоваването на подходящи или адаптирани защитни мерки и начините за получаване на копие или мястото, където са били предоставени.

Освен това е задължително тази информация да бъде предадена:

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

• веднага след събирането на данните, ако те се събират директно от служителя (например, когато са наети);

• до един месец след събирането, ако данните се събират индиректно от друг източник.

Тази информация обаче не е необходимо да се предоставя, ако служителят вече я има.

Забележка:

По отношение на взаимоотношенията между компанията и нейните служители, CNIL препоръчва да ги информират, когато те бъдат потърсени за информация (примери: актуализиране на административни данни, заявка за обучение, формуляр за поддръжка). оценка и др.) или при създаване на система за мониторинг, според процедурите, които се определят според организацията на фирмата (издаване на служебна бележка, изменение на трудовия договор, информация за интранет, приложена пощенска разписка и др.).

13) Гарантиране и засилване на правата на служителите върху техните данни: право на достъп, поправка, противопоставяне, заличаване (право да бъдат забравени), право на преносимост и ограничаване на обработката на лични данни.

GDPR налага да се предоставят на служителите средства за ефективно упражняване на правата им чрез контактна форма на уебсайт, телефонен номер или имейл адрес.

Правото да бъде забравеноа / заличена информацията е правото човек да получи от администратора възможно най-бързо изтриване на лични данни, отнасящи се до него / нея. Основанията, обосноваващи упражняването на това право, са изчерпателно изброени в член 17 от ППЗСР. По принцип GDPR налага да се пристъпи към изтриване на данните, тъй като те вече не са полезни по отношение на целите, за които са били събрани. Препоръчва се извън установяването на срокове за изтриване на данни, осигуряване на механизми за автоматично премахване или сигнали за инструментите, използвани за задържане на файлове. По-специално що се отнася до наемането на персонал, информацията за неуспешните кандидати трябва да бъде заличена, освен ако не са съгласни да останат в „пула“ на компанията (период на задържане ограничен до 2 години).

Правото на ограничаване на третирането означава правото на човек да поиска администраторът на данни да не използва определени събрани данни.

Правото на преносимост, което е новост, въведено от GDPR, е правото дадено лице да получи или дори да използва повторно данните, касаещи него, за личните си нужди, но то включва изпълнението на 3 условия:

• личните данни са предоставени от самото лице;

• данните се обработват автоматично, въз основа на съгласието на заинтересованото лице или за изпълнение на договор;

• преносимостта не трябва да нарушава правата и свободите на другите.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

14) Сигурността на данните е насочена към мерките, които трябва да бъдат предприети, виртуални или физически, и зависи от чувствителността на третираните данни и рисковете, които грозят хората в случай на инцидент.

Трябва да се изпълняват различни действия: антивирусни и софтуерни актуализации, редовна промяна на пароли и използване на сложни пароли или криптиране на данни в определени ситуации.

Компанията, която е станала жертва на нарушение на данните (личните данни са били случайно или незаконно унищожени, изгубени, променени, разкрити или неоторизиран достъп до данни) трябва да бъдат докладвани на CNIL в рамките на 72 часа, ако това нарушение е вероятно да представлява риск за правата и свободите на засегнатите лица. Това уведомление се прави онлайн на уебсайта на CNIL.

Субектът /ите на данните също трябва да бъдат уведомени, че техните данни са потенциално застрашени.

Забележка:

Ако не е възможно да се определи точно кой може да бъде засегнат от нарушения на сигурността, обществеността трябва да бъде уведомена за това, което може да бъде много сериозно от гледна точка на имиджа.

15) Рамка и засилване на мащаба на санкциите, предполагащи, че администраторите и подизпълнителите могат да бъдат обект на важни административни санкции в случай на игнориране на разпоредбите на регламента: предупреждение, официално предизвестие, разпореждане за спиране на обработката, спиране потоци от данни и т.н.

Административните глоби могат да бъдат, в зависимост от категорията на нарушението, между 10 и 20 милиона евро или, в случай на компания, от 2% до 4% от годишния глобален оборот. , като се задържа най-голямата сума.

Последната сума трябва да бъде свързана с факта, че за транснационална обработка санкцията ще бъде приета съвместно от всички съответни регулаторни органи, като по този начин е възможно за територията на целия Европейски съюз.

В този случай на дружеството ще бъде наложено едно и също решение за санкция, взето от няколко органа за защита.

16) Контролът, упражнен от CNIL за спазване на GDPR от 25 май 2018 г. 23, се състои в извършване на проверки в помещенията на организациите, онлайн, на изслушване и на документи. Процедурите за задействане на контрол също остават същите: решението за извършване на контрол ще се основава на годишната програма за контрол, жалби, получени от CNIL, информация, съдържаща се в медиите, или след прецедентен контрол.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Основната новост се състои във факта, че контролът, осъществяван върху международни участници, ще се извършва в контекста на много силно сътрудничество, което ще доведе до хармонизирано решение с европейски обхват.

Основните принципи за защита на данните остават до голяма степен непроменени (справедливост на обработката, уместност на данните, период на запазване, сигурност на данните и др.). Следователно те ще продължат да бъдат строго проверявани от CNIL.

От друга страна, по отношение на нови задължения или нови права, произтичащи от GDPR (право на преносимост, оценки на въздействието и т.н.), контролът, който ще бъде извършен, ще бъде основно предназначен като първа стъпка за подкрепа на компаниите в добро разбиране и оперативно изпълнение на текстовете. При наличието на добросъвестни организации, ангажирани в процеса на спазване и показващи сътрудничество с CNIL, този контрол обикновено не води до санкциониране по тези въпроси.

КАЗУС 2 - ФРАНЦИЯ

Предговор

От 1 септември 2017 г. колективните трудови договори трябва да бъдат публично оповестени и публикувани в национална база данни, достъпна чрез Интернет на следния адрес

https://www.legifrance.gouv.fr/initRechAccordsEntreprise.do

Целта на тази национална база данни е да улесни достъпа до разпоредбите, съдържащи се в колективните договори и колективните споразумения и по този начин да засили ролята на договарянето на предприятията.

1) Споразумения, предмет на това ново задължение за публикуване

Споразуменията и колективните споразумения, сключени след 1 септември 2017 г., трябва да бъдат публично достояние и поставени в национална база данни, достъпна от Légifrance. Това задължение се прилага независимо от степента на договаряне: компания, учреждение, междуфирмено дружество, група или клон.

Забележка:

Прилага се член L2231-5-1 от Кодекса на труда, който предвижда:

«Клоновите, груповите, B2B, корпоративните и търговските договори и споразумения се оповестяват публично и се въвеждат в национална база данни, съдържанието на които се публикува онлайн в лесно използваем отворен стандарт.

След сключването на договора или споразумението страните могат да се споразумеят, че част от договора или споразумението не се публикува, както е предвидено в първия параграф. Този акт, заедно с пълния текст на договора или споразумението и версията

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

на договора или споразумението, предназначени за публикуване, са приложени към депозита, предвиден в член L. 2231-6. При липса на такъв акт, ако някоя от организациите подписали това поиска, договорът или споразумението се публикуват в анонимен вариант, при условията, определени с постановление на Държавния съвет.

Условията за прилагане на този член са определени с Решение на Държавния съвет.

По изключение от 1 април 2018 г. колективните трудови договори, спестовните планове на служителите (споделяне на печалба, участие, спестовни планове на фирмата, B2B планове и Perco), както и споразуменията, определящи съдържанието на ESP, не подлежат на изискване за публикуване.

Това задължение обаче се прилага за конвенционалните колективни договори за прекратяване, въпреки че те включват икономическа и социална информация за компанията.

2) Възможността за публикуване в анонимен вариант

Съгласно членове L 2231-5-1 и D 2231-7 от Кодекса на труда, страната, отговорна за подаването на споразумение или конвенция, има задължението да приложи към него публикувана версия на споразумението или колективния договор в лесно използваем компютърен формат.

Тази версия трябва да е анонимна, тоест експурсирани имена и имена на преговарящите и на подписалия. Името на компанията, нейният номер SIREN, името на подписалите синдикални организации и качеството на техните представители трябва да бъдат включени в договора или споразумението.

След получаване на депозитния файл, Дирекцията изпраща публикуваната версия на текста до Дирекцията за правна и административна информация (DILA) за публикуване на уебсайта (www.teleaccords.travail-emploi.gouv.fr).

3) Документите, които ще бъдат депозирани

Независимо дали става въпрос за пълна или частична публикация, лицето, което подава споразумението или споразумението, трябва да приложи следните документи към подаването:

- пълната и подписана версия на споразумението;

- анонимната му публикувана версия;

- копие от писмото, имейл или разписка или потвърждение за получаване с дата на уведомяване на текста до всички представителни съюзи в края на процедурата за подписване.

В допълнение, в някои специални случаи трябва да се предостави допълнителна информация и документи:

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

- когато дружеството има отделни места, подаденият текст се придружава от списък на тези заведения и съответните им адреси;

- когато страните решат някои части от споразумението да не бъдат публикувани, те трябва да приложат частична публикация;

- по отношение на споразуменията, представени на референдум, протоколът от резултата от консултацията трябва да бъде приложен;

- подаването на допълнителни документи е необходимо и в конкретни случаи (пример: споразумение за действителните заплати).

За предпочитане тези документи се подават в PDF формат, с изключение на публикуваната версия на споразумението, която трябва да бъде във формат docx (www.teleaccords.travail-emploi.gouv.fr).

Забележка:

Списъкът на документите, които трябва да придружават подаването на споразумението или колективния трудов договор, е посочен в член D 2231-7 от Кодекса на труда.

4) Възможности за частично публикуване

Член L 2231-5-1 от Кодекса на труда позволява на подписващите група, междуфирмено предприятие, предприятие или учредяване на споразумение да решат, след като споразумението е сключено, да не публикуват определени части от него.

Това решение за частично публикуване обаче трябва да бъде формализирано с мотивиран и подписан акт:

- страна на служителите: с мнозинството в броя на подписалите синдикални организации

- от страна на работодателя: от законния представител на групата, предприятието или учреждението за споразуменията, сключени на тези нива, и от законните представители на съответните дружества за споразумения за бизнес (прилага се член R 2231) - 1-1 от Кодекса на труда).

Актът за частична публикация, публикуваната версия на текста и подписаната пълна версия са приложени към подаването.

Колективният договор или споразумението ще бъдат публикувани с указанието, че публикацията е частична.

Забележка:

От 1 април 2018 г. секторните, професионалните или междупрофесионалните споразумения вече не могат да се възползват от тази възможност; те трябва да бъдат публикувани изцяло.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

5) Въпроси, които все още са висящи

Остават обаче въпроси относно естеството на акта за публикуване.

Тъй като актът за частично публикуване не е колективен договор, неговото договаряне не би било предмет на общото право на колективното договаряне и би засягало само синдикалните организации, подписали споразумението (в този смисъл RJS 11/18 783 Jeansen and Thuleau, " Публичност на колективните договори между прозрачност и секретност “).

И накрая, нито законът, нито регулаторните разпоредби определят условията за приемане на акта за частично публикуване в случай на споразумение, сключено с представители на персонала, които не са упълномощени от синдикални организации или ратифицирани от 2/3 от персонала въз основа на предложение от работодателя. Такъв акт не изглежда възможен за тези споразумения по отношение на условията за подписване, предвидени в текстовете.

За момента обаче не е предвиденното един текст на закона, който да разреши тези въпроси и да даде отговори на въпросите, които те предизвикват.

6) Защита на интересите на компанията

Чрез едностранно решение работодателят може да скрие елементите, засягащи стратегическите интереси на компанията.

Той използва текста, предложен от член L 2231-5-1 от Кодекса на труда.

Този вариант е особено интересен за споразумения, чиито процедури за приемане не позволяват сключването на частично публикуване.

КАЗУС 3 - ФРАНЦИЯ

Предговор

Икономическият и Социален Комитет / CSE и синдикатите на служителите все още чакат изготвянето на GDPR стандартите от Националната комисия по информация и защита на личните свободи (CNIL). Междувременно CNIL остава гъвкав по отношение на спазването им.

Преди прилагането на Европейския общ регламент за защита на личните данни (GDPR) във Франция, Социалният и икономически комитет на дружество или предприятие получи освобождаване от декларацията за лични данни на Националния институт по изчислителни и свободи на Комисията (CNIL). Но от 25 май 2018 г., влизането в сила на GDPR, тези разпоредби на CNIL вече нямат правна стойност.

Днес защитата на данните, обусловена от GDPR, също е насочена към CSE. В действителност, в рамките на своите мисии и признания (по-специално за социалните и културни действия), CSE се предлага за събиране и обработка на лични данни, по-

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

специално данните на служителите, свързани със семейния и личния им живот, както и тяхното здраве: фамилия, име, адрес, фамилна ситуация, функция, телефонен номер и адрес на електронна поща, здравословно състояние, социални и културни дейности и др. Освен това, определено количество лична информация, свързана със служителите, се предава към него в контекста на задължителните консултации (възнаграждение и т.н.).

Следователно CSE трябва да се съобразява с GDPR по отношение на обработката на тези данни:

- Събирайте съгласието на служителите относно обработването на личните им данни;

- Информиране на служителите за техните права;

- Прилагане на подходящи технически и организационни мерки, за да се гарантира и може да се докаже, че обработката се извършва в съответствие с;

- Водете регистър на обработката на лични данни;

- Планиране на мерки за осигуряване на поверителност на обработваните данни;

- Назначаване на делегат за защита на личните данни в рамките на CSE.

В резултат на това ИСС трябва да определи точни правила за всички събрани лични данни и да ги направи публично достояние на служителите. След това CSE трябва да защитава цялата си информация. Той трябва да гарантира служителите, че няма да бъдат достъпни за неоторизирани лица. CSE също така се задължава да не злоупотребява с тези данни. С други думи, всеки от тях има цел. CSE няма право да използва тези данни за други цели. Трябва да е било упълномощено от съответното лице или лица.

Прогресивно прилагане на регистъра на лечебните дейности

Член 30 от GDPR, предвижда създаването на регистър на дейностите по обработка. Този регистър дава възможност да се регистрира обработката на данни и да се направи преглед на това, което CSE прави с личните данни. Това е документ, в който ще бъдат записани всички лични данни. Като пример, CNIL предлага модел на регистър (допълнение 1). Форматът на този документ е безплатен. Тя може да бъде цифрово проектирана или представена в по-ръкописна форма. Този регистър е инструмент за пилотиране и доказване на съответствието на CSE с GDPR.

Регистърът на дейностите по обработка на данни дава възможност да се регистрира обработката на данни и да се направи преглед на личните данни.

3 стъпки за разработване на данните за лечебните дейности:

- Назначаване на делегат за защита на лечения,

- Регистрация и групова обработка на данни по дейности,

- Попълнете всеки лист за дейности, в който подробно се обработват данните.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Ролята на служителя по защита на данните (DPO)

За да актуализира регистъра на дейностите по обработка на лични данни и да гарантира спазването на GDPR, CSE може да назначи служител по защита на данните (DPO).

Тази мярка не е задължителна, но силно се препоръчва при компании, управляващи много лични данни. Назначаването на DPO може да бъде полезно в контекста на информационно-консултативната мисия на CSE пред администратора или подизпълнителя.

Понастоящем няма допълнително време за делегиране на служителя по защита на данните. Страхува се, че тази нова система ще доведе до малко повече отговорност и натоварване на избраните представители, особено на определения делегат. Тази работа вероятно ще отнеме време, особено през следващите месеци, докато за много избрани служители преминаването към CSE е в ход.

Съгласието на служителя

GDPR поставя като условие да иска съгласието на служителите за събиране на тяхната информация. Представителите на персонала трябва да определят как да получат това споразумение, независимо дали става въпрос за документ, написан и подписан от служителя, или дори квадратче за отметка, когато се консултирате с уебсайта. Във всеки случай използваните средства трябва ясно да показват на субекта на данните, че той приема обработването на своите данни.

По този начин служителите могат да изискват от CSE:

- достъп до информация, която ги засяга;

- коригиране на личните им данни;

- изтриването на техния профил, ако е необходимо.

За тази цел CSE трябва ясно да обясни на служителите процедурата / процедурите, които трябва да следват. Именно при това условие най-добре ще се спазва регулацията.

ИСС има задължението да въведе вътрешни разпоредби, които да определят нейните оперативни процедури, нейните правила и тези на отношенията му със служителите за изпълнение на мисиите му. За да бъдат в съответствие, голям брой ЕО / ЕСС включват в процедурния правилник специална клауза за защита на данните.

Информационното консултиране на CSE при прилагането на RGPD

Работодателите и отделите за човешки ресурси също трябва да се съобразяват с третирането на личните данни на служителите. Като такъв, избраният CSE може да бъде поискан в съответствие с компанията. Това може да стане по-специално чрез информационно консултиране на CSE (по-специално при извършване на анализ на въздействието на конкретно лечение) и / или подписване на фирмено споразумение, по-специално с управителите на магазина.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Примери за възможно участие на синдикати и представители на персонала:

- Компютърна харта (и контрол на използването на компютърна техника от служителите);

- Вътрешни разпоредби (контрол на достъпа до помещения, видеонаблюдение, геолокация, използване на телефон, контрол на работното време, използване на значки, кодекс за поведение и др.);

- Споразумение за предаване на лични данни между компанията и CSE.

Тези практики не са задължителни, но се препоръчват, за да позволят на компанията постепенно спазване, без вътрешни конфликти.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057