

- Член 16 от Договора за функционирането на Европейския съюз (предишен член 286 от Договора за създаване на Европейската общност) посочва, че „всеки има право на защита на неговите лични данни“ и изисква да се определят правила за защита на физическите лица по отношение на обработката на личните им данни и свободното движение на данни. Тези норми се прилагат за институциите и органите на ЕС, създадени със или основаващи се на Договора.
- Регламент 2018/1725 относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни има за цел да изпълни изискванията на Договора и да предостави на физическите лица гарантирани от закона права, да определи конкретните задължения на администраторите на лични данни във връзка с обработката на данни и да създаде независим надзорен орган.
- Целите на Регламент 2018/1725 са свързани със защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на ЕС, както и свободното движение на лични данни между тях или до други получатели, установени в ЕС. По-долу са посочени някои определения, засягащи защитата на личните данни и свързани с това теми, както и информация относно защитата на личните данни в Сметната палата:

Принципи за защита на данните

Администраторът носи отговорност за спазването на нормите и трябва да е в състояние да докаже това („отговорност“). Всяко лице, обработващо лични данни, следва да е информирано за някои основни принципи, които изискват тези данни:

- да се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;
- да се обработват за конкретни, изрично указани и законни цели („ограничаване в рамките на целта“);
- да са адекватни, относими и да не надхвърлят необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);
- да са точни и, при необходимост, поддържани в актуален вид („точност“);
- да се съхраняват за период, не по-дълъг от необходимия („ограничено съхраняване“);
- да се обработват по начин, който гарантира подходящо ниво на сигурност („цялостност и поверителност“);
- да не се предават на трети страни без въвеждане на подходящи защитни мерки;
- да се обработват при спазване на правата на субекта на данните.

Какво представляват личните данни?

- „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“).
- Физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез характеристики като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, икономическата, културната или социалната идентичност на това физическо лице.
- Забранява се обработването на специфични категории лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в професионални съюзи, както и обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравето или сексуалния живот и сексуалната ориентация на лицето, като са възможни някои изключения (вж. член 10 от Регламент 2018/1725).

Администратор на лични данни и субект на данни

„Администратор на лични данни“ означава институция или орган на ЕС, генерална дирекция, отдел или всяка друга организационна структура, която самостоятелно или съвместно с други структури определя целите и средствата за обработването на лични данни.

Администраторите на Сметната палата са нейните членове, генералният секретар, директорите и главните ръководители.

За всяка операция по обработка на данни следва да бъде определен администратор, както и да бъде изпратено предварително уведомление до служителя за защита на данните на институцията.

„Субект на данни“ е лицето, чиито лични данни се събират, съхраняват или обработват от администратора на лични данни.

Обработващо лице

Ако администраторът на лични данни не обработва сам данните, това се извършва от обработващо лице от името на администратора. Обработващото лице следва да предостави достатъчни гаранции по отношение на необходимите технически и организационни мерки за сигурност и да осигури изпълнението на тези мерки. Обработващото лице може да бъде физическо или юридическо лице, публичен орган, агенция или всеки друг орган, действащ само и единствено съгласно инструкциите на администратора на лични данни. Както администраторът, така и обработващото лице са обвързани с договор или друг правен акт, който урежда обработването на лични данни.

Лице за контакт (оправомощен контролиращ орган)

Лицето за контакт (или „оправомощен контролиращ орган“) се определя от администратора на лични данни и действа съгласно неговите инструкции. Задачата на лицето за контакт е да изготвя уведомленията, които се изпращат до длъжностното лице по защита на данните от отговорния администратор (след валидиране), както и да поддържа контакти с длъжностното лице по защита на данните, когато е необходимо.

Длъжностно лице по защита на данните

- Всяка институция разполага с едно или повече длъжностни лица по защита на данните, които следят независимо за спазването на принципите на защита на личните данни в институцията. Длъжностните лица поддържат регистър на всички операции за обработване на лични данни в съответната институция. Те също така предоставят консултации и изготвят препоръки по отношение на правата и задълженията. Длъжностните лица уведомяват Европейския надзорен орган по защита на данните в случаите, когато обработването на личните данни е свързано с елемент на риск (вж. по-долу), и отговарят на заявките от този орган. Те могат да разследват въпроси и инциденти по получена заявка или по собствена инициатива.

- От юни 2010 г. длъжностното лице по защита на данните на ЕСП е Johan Van Damme, подпомаган от Dominique Savonitto.

Какво е уведомление („запис на дейности по обработване“) и кой е отговорен за него?

- Уведомление е предварително съобщение, което администраторът на лични данни изпраща на длъжностното лице по защита на данните относно всяка (ръчна или електронна) обработка на лични данни. Такова уведомление се изисква само ако се обработват лични данни.

Какво е регистър на длъжностното лице по защита на данните?

- Регистърът е база данни, съдържаща всички уведомления, които администраторът е изпратил на длъжностното лице по защита на данните по отношение на обработката на лични данни. Член 31 от Регламент 2018/1725 изисква от длъжностните лица по защита на личните данни да поддържат регистър на дейностите по обработване, като този регистър следва да бъде публично достъпен.

Какво е документна система на лични данни?

- Регламент 2018/1725 се прилага във всички случаи, когато се обработват лични данни, които съставляват или са предназначени да съставляват част от документна система. „Документна система“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.
- Местоположението на системата не е от значение. Тя може да е създадена на ниво Сметна палата, но може да бъде и на институционално, национално, регионално, местно или дори „частно“ равнище (в одитирано дружество).

Какво е обработване?

„Обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства като събиране, записване, организиране, съхранение, консултиране, употреба, разкриване чрез предаване, изтриване, унищожаване и др.

Какво е законосъобразно обработване?

- Член 5 от Регламента посочва, че обработването на лични данни трябва да бъде необходимо или доброволно. Личните данни могат да бъдат обработвани само ако:

- а) обработването е необходимо за изпълнението на задача от обществен интерес съгласно законодателството на ЕС или при упражняването на официално правомощие, което е предоставено на институцията или органа на ЕС;
- б) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора на лични данни;

- с) обработването 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;
- д) субектът на данните недвусмислено е изразил своето съгласие (което означава всяко свободно изразено, конкретно и информирано указание за волята на субекта на данните, което изразява съгласието му свързаните с него лични данни да бъдат обработени);
- е) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните.
- Администраторът на лични данни следва да гарантира, че данните се обработват добросъвестно и законосъобразно.

Обхват

- Когато определена служба на Сметната палата обработва лични данни, съдържащи се в (електронен или физически) регистър, независимо къде се намира този регистър, какви данни съдържа той и за каква цел се извършва обработката, това се счита за обработване на лични данни по смисъла на Регламент 2018/1725. Регламент 2018/1725 се прилага и когато лични данни, предназначени да съставляват част от регистър, се обработват от служители на Сметната палата.
- Длъжностното лице по защита на данните следва да бъде уведомено за обработването чрез системата за уведомяване (регистър на дейностите по обработване), използвана в Сметната палата.

Информация, която следва да бъде предоставена на субекта на данните преди събирането на лични данни (член 15 от Регламент 2018/1725) и права на субекта на данните по отношение на обработката на личните му данни (членове 17—24 от Регламент 2018/1725)

- Субектът на данните има право да получи от администратора следната информация относно обработването на данните:
- самоличността и координатите за връзка на администратора
 - координатите за връзка на длъжностното лице по защита на данните
 - целите на обработването, за което са предназначени личните данни, както и правното основание за обработването
 - получателите или категориите получатели на личните данни, ако има такива
 - когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация [...], както и наличието или липсата на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 48, позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.
 - срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;
 - съществуването на право на достъп до личните данни и на тяхната корекция във възможно най-кратък срок, ако те са неточни или непълни.
 - съществуването на правото при определени условия да се поиска изтриване на личните данни или ограничаване на тяхното използване.
 - когато е приложимо, съществуването на право на възражение срещу обработването на личните данни по всяко време, по основания, свързани с конкретна ситуация, както и право на преносимост на данните.
 - съществуването на правото да се оттегли съгласието (когато обработката на личните данни се основава на доброволно съгласие)
 - съществуването на правото субектът да не бъде адресат на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за него или го засяга в значителна степен
 - съществуването на право да бъде подадена жалба до Европейския надзорен орган по защита на данните
 - дали предоставянето на лични данни е законоустановено или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и какви са евентуалните последици, ако тези данни не бъдат предоставени
 - дали администраторът възнамерява да обработва по-нататък личните данни за цел, различна от тази, за която са събрани, както и предоставяне на информация за тази друга цел и всякаква друга необходима информация (период на съхранение, права и др.)
 - съществуването на правото да се съобщи, доколкото е възможно, относно евентуални промени на личните данни на други страни, на които са били разкрити данните.

Заявките следва да се обработват във възможно най-кратък срок, но най-късно в рамките на един месец от получаването им. Ако е необходимо, този срок може да бъде удължен с още два месеца.

Европейски надзорен орган по защита на данните

- [Европейският надзорен орган по защита на данните](#) е независим надзорен орган, създаден в съответствие с Регламент 2018/1725. По отношение на обработването на лични данни задачата на Европейския надзорен орган по защита на данните е да гарантира спазването от страна на институциите и органите на ЕС на основните права и свободи на физическите лица, и по-специално правото им на неприкосновеност на личния живот. Европейският

надзорен орган по защита на данните също така консултира институциите и органите на ЕС по всички въпроси, засягащи обработката на лични данни.

- Администраторите на лични данни са длъжни да сътрудничат на Европейския надзорен орган, по-специално като му предоставят достъп до информация.