РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

01037/12/BG
WP 196

Становище 05/2012 относно изчислителните облаци (cloud computing)

Прието на 1 юли 2012 г.

Тази работна група бе създадена по силата на член 29 от Директива 95/46/ЕО. Тя е независим европейски съвещателен орган по защитата на личните данни и личния живот. Задачите ѝ са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът е осигурен от Дирекция С (Основни права и гражданство на Съюза) на Генерална дирекция „Правосъдие“ на Европейската комисия, B-1049, Брюксел, Белгия, Офис № MO-59 02/013.

Уебсайт: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Резюме

В настоящото становище Работната група по член 29, анализира всички важни въпроси, свързани с работещите в Европейското икономическо пространство (ЕИП) доставчици на услуги в изчислителните облаци и техните клиенти, като посочва всички приложими принципи от Директивата на ЕС за защита на личните данни (95/46/ЕО) и Директивата за правото на неприкосновеност на личния живот и електронните комуникации 2002/58/ЕО (заедно с измененията в 2009/136/ЕО), където това е уместно.

Въпреки установените ползи от изчислителните облаци и в икономически, и в социален аспект, настоящото становище показва, как широкото разгръщане на услугите в изчислителните облаци може да доведе до редица рискове по отношение на защитата на лични данни, най-вече до липсата на контрол над личните данни, както и до наличието на недостатъчна информация по отношение на това как, къде и от кого се обработват/дообработват данните. Тези рискове трябва да бъдат внимателно оценени от страна на държавните органи и частните предприятия, когато те обмислят да използват услугите на доставчици на услуги в изчислителните облаци. Настоящото становище разглежда въпроси, свързани със споделянето на ресурси с трети страни, липсата на прозрачност в дадена аутсорсинг верига, състояща се от множество обработващи и подизпълнители, липсата на обща глобална рамка за преносимост на данните и несигурността по отношение на допустимостта на трансфера на лични данни към доставчиците на услуги в изчислителните облаци, които са установени извън границите на ЕИП. Също така, в становището се отбелязва, че сериозно безпокойство буди липсата на прозрачност по отношение на информацията, която един администратор на данни е в състояние да предостави на субектите на данните относно начина на обработка на личните им данни. Субектите на данни трябва[1] да са информирани за това, кой и за какви цели обработва техните данни и да са в състояние да упражнят правата, които имат в това отношение.

Основното заключение на настоящото становище е, че предприятията и администрациите, които искат да използват изчислителни облаци, като първа стъпка трябва да извършат цялостен и задълбочен анализ на риска. Всички доставчици, предлагащи услуги в изчислителните облаци в ЕИП, следва да предоставят на клиента в изчислителния облак цялата информация, необходима за правилната оценка на плюсовете и минусите за приемане на такива услуги. Основните фактори за клиента при вземане на решения относно оферти за услуги в изчислителните облаци трябва да са сигурността, прозрачността и правната сигурност.

По отношение на препоръките, съдържащи се в настоящото становище, тук се поставя акцент върху отговорностите на клиентите на услуги в изчислителните облаци в качеството им на администратори на данни като се препоръчва клиентът да избере такъв доставчик на услуги в изчислителни облаци, който гарантира спазването на законодателството на ЕС за защита на личните данни. В становището са разгледани съответни предпазни договорни клаузи и се поставя изискването, всеки договор между клиент и доставчик на услуги в изчислителните облаци да дава достатъчно гаранции по отношение на техническите и организационните мерки. Също така от значение е

[1] Ключовите думи „ТРЯБВА”, „НЕ БИВА”, „НЕОБХОДИМО”, „ДЛЪЖЕН(А) Е”, „НЯМА”, „БИ БИЛО ДОБРЕ”, „НЕ БИ ТРЯБВАЛО”, „ПРЕПОРЪЧАНО”, „МОЖЕ” и „ПО ИЗБОР” в този документ ще имат смисъла, определен в Заявление за обсъждане 2119. Документът може да се намери на http://www.ietf.org/rfc/rfc2119.txt. Въпреки това, за целите на осигуряване на яснота на документа, в тази спецификация тези думи не са използвани с главни букви.

препоръката, клиентите на услуги в изчислителните облаци да проверят дали доставчиците на услугите могат да гарантира законосъобразността на всички трансгранични международни трансфери на данни.

Както всеки еволюционен процес, развитието на изчислителните облаци като глобална технологична парадигма представлява предизвикателство. Настоящото становище, в сегашния му вид, може да се счита за важна стъпка в определянето на задачите, които трябва да се приемат в това отношение от страна на Общността през следващите години с цел да се осигури защита на данните.

Съдържание

1. Въведение

Някои хора считат изчислителните облаци за една от най-големите технологични революции, появили се в последно време. За други, това е само естествена еволюция на набор от технологии, целящи да се постигне дългоочакваната мечта за търгуване на пакети от изчислителни ресурси. Във всеки случай, много от заинтересованите страни са поставили изчислителните облаци на преден план в развитието на технологичните си стратегии.

Изчислителният облак се състои от набор от технологии и модели на обслужване, които се фокусират върху Интернет-базираното използване и предоставянето на ИТ приложения, възможности за обработка, съхранение и памет. Изчислителните облаци могат да генерират значителни икономически ползи, тъй като използваните само при нужда ресурси могат съвсем лесно да бъдат конфигурирани, разширени и достъпни в Интернет. Заедно с икономическите ползи, изчислителните облаци могат да допринесат за повишаване на сигурността; предприятията, особено малките и средни предприятия, могат да придобият на маргинални цени първокласни технологии, които иначе биха били извън тяхната бюджетна рамка.

Доставчиците на услуги в изчислителните облаци предлагат широка гама от услуги, вариращи от виртуални системи за обработка (които заменят и/или работят заедно с конвенционалните сървъри под прекия контрол на администратора) и услуги, поддържащи разработката на приложения и разширен хостинг, до уеб-базирани софтуерни решения, които могат да заменят приложенията и са условно инсталирани на персоналните компютри на крайните потребители. Това включва приложения за текстова обработка, дневни програми и календари, архивиращи системи за онлайн съхранение на документи и външни услуги за електронна поща. Някои от най-често използваните определения за тези различни видове услуги са включени в приложението към настоящото становище.

В това становище Работната група по член 29 (наричана по-нататък за краткост „РГ по чл. 29”) анализира приложимото законодателство и задълженията на администраторите на данни в Европейското икономическо пространство (наричано по-нататък за краткост „ЕИП”) и за доставчиците на услуги в изчислителните облаци за клиенти в ЕИП. Това становище се фокусира върху ситуацията, при която се предполага, че връзката е от типа администратор-обработващ, при което клиентът се квалифицира като администратор на данни, а доставчикът на услуги в изчислителните облаци – като обработващ данните. В случаите, когато доставчикът на услуги в изчислителните облаци действа и като администратор на данни, той трябва да отговаря на допълнителни изисквания. Като следствие от това и за да се осигури надеждност на изчислителните облаци се налага изискването за администратора на данни да извърши адекватна оценка на риска, включително и на местоположението на сървърите, които обработват данните, както и разглеждане на рисковете и ползите от гледна точка на защитата на данните съгласно критериите, описани в параграфите по-долу.

Настоящото становище посочва приложимите принципи, както за администраторите, така и за обработващите, съдържащи се в директивата за обща защита на данните (95/46/ЕО), като например определяне и ограничаване на целта, заличаване на данните и съответните технически и организационни мерки. Становището дава насоки за изискванията за сигурност, както като структурни, така и като процедурни предпазни мерки. Специален акцент е поставен върху договорни споразумения, които трябва да регулират отношенията между администратора на данни и обработващия данните в

тази връзка. Класическите цели на сигурността на данните включват тяхната достъпност, достоверност и поверителност. Защитата на данните, обаче, не се ограничава само до сигурността на данните и следователно тези цели са допълнени със специфичните за защитата на данните цели като прозрачност, изолация, възможност за интервенция и преносимост, които са в подкрепа на правата на лицата за защита на техните данни, залегнали в чл. 8 от Хартата на ЕС за основните права.

По отношение на прехвърлянето на лични данни извън ЕИП, се анализират такива инструменти, като стандартните договорни клаузи, приети от Европейската комисия, констатациите относно адекватността и евентуалното лице, което ще обработва данните – задължителните корпоративни правила (BCR), както и рисковете за защита на данните, произтичащи от исканията на международните правоприлагащи органи.

Това мнение завършва с препоръки към клиентите на услуги в изчислителните облаци в качеството им на администратори на данни, към доставчиците на услуги в облака в качеството им на обработващи данните лица и към Европейската комисия за бъдещи промени в европейска рамка за защита на данните.

Берлинската Международна работна група за защита на данните в телекомуникациите прие през април 2012 г. *Сопотския меморандум*[2]. Меморандумът разглежда въпросите, свързани със защитата на личния живот и личните данни в изчислителните облаци и подчертава, че изчислителните облаци не трябва да води до понижаване на стандартите за защита на данните, в сравнение с конвенционалната обработка на данни.

2. Рискове за защитата на личните данни, произтичащи от изчислителните облаци

Тъй като настоящото становище се фокусира върху обработката на лични данни в изчислителните облаци, тук са разгледани само специфичните рискове, свързани с този контекст.[3] По-голямата част от тези рискове попадат в две основни категории, а именно: липсата на контрол върху данните и недостатъчната информация относно обработката (липса на прозрачност). Специфичните рискове в изчислителните облаци, разгледани в настоящото становище, включват:

Липса на контрол

С предоставяне на лични данни в системи, управлявани от доставчик на услуги в изчислителни облаци, клиентите в облака вече не могат да осъществяват изключителен контрол над тези данни и не могат да наложат техническите и организационните мерки, необходими за осигуряване на достъпността, достоверността, поверителността, прозрачността, изолацията[4], възможността за намеса и преносимостта на данните. Тази липса на контрол може да се прояви по следния начин:

- Недостъпност поради липса на оперативна съвместимост (зависимост на клиента от доставчика на услугата): ако доставчикът на услуги в облака използва патентована технология, за клиента в облака може да се окаже трудно да прехвърля данни и документи между различните системи в облака (преносимост

[2] http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

[3] В допълнение към изрично посочените в настоящото становище рискове, свързани с обработваните „в облака" лични данни, трябва също така да се вземат под внимание и всички рискове, свързани с аутсорсинг на обработката на лични данни.

[4] В Германия е въведена по-широкото понятие за „несвързаност". Вж. бележка 24 по-долу.

на данните) или да размени информация с лица, които използват услуги в облака, управлявани от различни доставчици (оперативна съвместимост).

- Нарушаване на достоверността поради споделяне на ресурси: облакът се състои от споделени системи и инфраструктури. Доставчиците на услуги в изчислителните облаци обработват лични данни, получени от голям брой източници, включващи субекти на данни и организации, което позволява възникването на конфликти на интереси и/или различни цели.
- Нарушаване на поверителността в случай на искания от правоприлагащите органи, отпратени директно към доставчика на услуги в облака: личните данни, обработвани в облака, могат да са предмет на искания на правоприлагащите органи на държавите-членки на ЕС и на трети страни. Съществува риск, че личните данни могат да бъдат разкривани на (чужди) правоприлагащи органи без валидно правно основание съгласно нормативната уредба на ЕС и по този начин да се наруши законодателството на ЕС за защита на личните данни.
- Липса на възможност за интервенция поради сложността и динамиката на аутсорсинг веригата: услугите в облака, предлагани от един доставчик, могат да представляват комбиниране на услуги от голям брой други доставчици, които евентуално могат да бъдат динамично добавени или премахнати по време на срока на действието на договора с клиента.
- Липса на възможност за интервенция (права на субектите на данни): доставчикът на услуги в облака може да не е в състояние да предостави необходимите мерки и инструменти за подпомагане на администратора на данни по отношение например на достъпа, заличаването или коригирането на данните.
- Липса на изолация: доставчик на услуги в облака може да използва физически контрол върху данни от различни клиенти, за да свърже отделни лични данни. Ако администраторите са улеснени с достатъчно привилегировани права на достъп (високо-рискови роли), те могат да свързват информация от различни клиенти.

Липса на информация за обработка (прозрачност)

Недостатъчната информация за операциите по обработка в изчислителните облаци представлява риск и за администраторите, и за субектите на данни, тъй като те потенциално могат да не са наясно с потенциалните заплахи и рискове и по този начин да не могат да вземат мерките, които считат за подходящи.

Някои от потенциалните заплахи, които могат да възникнат от факта, че администраторът не е информиран за следното:

- Извършване на верижна обработка с участието на множество обработващи и подизпълнители.
- Обработване на лични данни в различни географски местоположения в рамките на ЕИП. Това се отразява директно върху законодателството за защита на данните, приложимо при всички спорове, които могат да възникнат между потребителите и доставчиците.
- Прехвърляне на лични данни към трети страни, извън ЕИП. Третите страни не могат да предоставят адекватно ниво на защита на данните и трансферите не могат да бъдат защитени чрез подходящи мерки (например стандартни договорни клаузи или задължителни корпоративни правила) и по този начин те могат да се окажат незаконни.

Съществува изискване, което гласи, че субектите на данни, чиито лични данни се обработват в облака, трябва да са информирани за самоличността на администратора

на данни и целите на обработването (съществуващо изискване за всички администратори съгласно Директивата за защита на данните 95/46/ЕО). Предвид потенциалната сложност на обработващите вериги в средата на изчислителния облак, с цел гарантиране на справедливост на обработката на данните по отношение на субекта на данни (чл. 10 от Директива 95/46/ЕО), като въпрос на добра практика администраторите на лични данни трябва да предоставят допълнителна информация, свързана с (под-)обработващите лица, предоставящи услуги в облака.

3. Правна рамка

3.1 Рамка за защита на личните данни

Приложимата правна рамка е Директива 95/46/ЕО за защита на данните. Тази директива се прилага във всички случаи, включващи обработка на лични данни в резултат на използване на услуги в изчислителните облаци. Директивата за правото на неприкосновеност на личния живот и електронните комуникации 2002/58/ЕО (заедно с измененията в 2009/136/ЕО) се прилага по отношение на обработката на лични данни във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи (телекомуникационни оператори) и по този начин е приложима, когато тези услуги се предоставят посредством решения в изчислителни облаци[5].

3.2 Приложимо право

Критериите за установяване на приложимостта на законодателството се съдържат в чл. 4 от Директива 95/46/ЕО, която се позовава на нормативните актове, приложими за администратори на данни[6] с едно или повече места на установяване в рамките на ЕИП, а също и на нормативните актове, приложими за администратори на данни, които са установени извън ЕИП, но за обработка на лични данни използват оборудване, разположено в рамките на ЕИП. Работната група по член 29 анализира този въпрос в своето Становище 8/2010 относно приложимото право[7].

В първия случай, факторът, който определя прилагането на правото на ЕС спрямо администратора е мястото, където той е установен, както и дейностите, които извършва в съответствие с член 4.1.а) от директивата, при което видът на модела услуги в облака е без значение. Приложимото законодателство е законът на страната, в която е установен администраторът, договорил услуги в изчислителни облаци, а не мястото, в което се намират доставчиците на услуги в изчислителни облаци.

[5] Директива 2002/58/ЕО за правото на неприкосновеност на личния живот и електронните комуникации (заедно с измененията в Директива 2009/136/ЕО): Директива 2002/58/ЕО за правото на неприкосновеност на личния живот в областта на телекомуникациите се отнася за доставчиците на електронни съобщителни услуги, достъпни за обществеността, като изисква от тях да гарантират изпълнението на задълженията, свързани с тайната на комуникациите и защитата на личните данни, както и правата и задълженията по отношение на електронните съобщителни мрежи и услуги. В случаите, когато доставчиците на услуги в изчислителните облаци действат като доставчици на публично достъпни електронни съобщителни услуги, те попадат в обхвата на този регламент.

[6] Понятието за администратор на лични данни е дадена в чл. 2(з) от директивата и бе анализирано от РГ по член 29 в нейното Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните".

[7] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

Ако администраторът е установен в различни държави-членки и обработва данни като част от своята дейност в тези страни, приложимо ще е правото на всяка от държавите-членки, в които се осъществява тази обработка на данни.

Чл. 4.1(в)[8] се отнася за това, как се прилага законодателството за защита на данните спрямо администраторите, които не са установени в ЕИП, но използват автоматизирано или друго оборудване, разположено на територията на държава-членка, освен в случаите, когато това оборудване се използва само за целите на транзитно преминаване. Това означава, че ако клиент в облака е установен извън ЕИП, но използва доставчик на услуги в облак, установен в ЕИП, тогава доставчикът следва да прилага законодателството за защита на данните на клиента.

3.3 Задължения и отговорности на различните участници

Както вече беше посочено, изчислителните облаци включват набор от различни участници. Важно е да се оцени и изясни ролята на всеки един от тези участници, за да се установят специфичните им задължения във връзка с действащото приложимо законодателство за защита на личните данни.

Следва да се припомни, че в своето становище 1/2010 относно понятията „администратор" и „обработващ" РГ по чл. 29 посочва, че „*първата и основна роля на концепцията на администратора е да определи кой ще носи отговорност за спазването на правилата за защитата на данните и начина, по който субектите на данни могат да упражняват правата си на практика. С други думи: да разпредели отговорностите*." Страните, участващи във въпросния анализ, трябва да имат предвид тези два общи критерия за отговорността за спазването и разпределението на отговорностите.

3.3.1 Клиент в облака и доставчик в облака

Клиентът в облака определя крайната цел на обработването на данни и взема решение за възлагането на това обработване и делегирането на всички или на част от дейностите по обработване на външна организация. Следователно, клиентът в облака действа като администратор на данни. Директивата определя администратора като „*физическо или юридическо лице, държавен орган, агенция или друг орган, който сам или съвместно с други определя целите и средствата на обработка на лични данни"*. Клиентът в облака, в качеството си на администратор на лични данни, трябва да поеме отговорността за съблюдаването на законите за защита на данните, при което носи отговорност и подлежи на всички законови задължения, разгледани в Директива 95/46/ЕО. Клиентът в облака може да възложи на доставчика на услуги в облака избора на методи и технически или организационни мерки, необходими за постигане за целите на администратора.

Доставчикът на услуги в облака е лице, което предоставя услуги в изчислителните облаци в различните форми, които бяха обсъдени по-горе. Когато доставчикът на услуги в облака предоставя средства и платформа, действайки от името на клиента в облака, то тогава той се счита за лице, обработващо данните, т.е. в съответствие с

[8] Член 4(1)(в) гласи, че законодателството на съответната държава-членка ще е приложимо, когато „администраторът не е установен на територията на Общността, и за целите на обработването на лични данни използва автоматизирано или друго оборудване, намиращо се на територията на дадената държава-членка, освен ако оборудването се използва само за целите на транзитното преминаване през територията на Общността".

Директива 95/46/ЕО „*физическо или юридическо лице, държавен орган, агенция или друг орган, който обработва личните данни от името на администратора*”.[9][10]

Както е посочено в Становище 1/2010, за оценка на контрола на обработването могат да се използват няколко критерия[11]. В действителност може да съществуват ситуации, в които един доставчик на услуги в облака може да се разглежда като съвместен администратор или като самостоятелен администратор в зависимост от конкретните обстоятелства. Например, такъв може да е случаят, когато доставчикът обработва данни за свои собствени цели.

Трябва да се подчертае, че дори и в сложни среди за обработка на данни, където в обработването на лични данни участват различни администратори, ясно трябва да се установи спазването на правилата за защита на данните и отговорността за евентуални нарушения на тези правила, за да не се допусне намаляване на нивото на защита на личните данни или възникване на „негативен конфликт на компетентност” и пропуски, при което някои задължения или права, произтичащи от директивата, не се осигуряват по отношение на някоя от страните.

В сегашния вариант на изчислителни облаци, клиентите на услуги в облака могат да не разполагат с възможност за маневриране при договарянето на условията за използване на услугите в облака, тъй като много услуги в изчислителните облаци се предлагат като стандартизирани оферти. Въпреки това, в крайна сметка клиентът взема решението за разпределяне на част или всички операции по обработване на данни като облачни услуги за специфични цели; ролята на доставчика на услуги в облака ще е на изпълнител по отношение на клиента, което е ключовият момент в този случай. Както е посочено в Становище 1/2010[12] на Работна група по член 29 относно понятията „администратор на лични данни” и „лице, което обработва данните”, „*дисбалансът между договорните правомощия на един малък администратор на данни в сравнение с тези на големите доставчиците на услуги не трябва да се разглежда като оправдание за администратора да приема клаузи и договорни условия, които не са в съответствие със законодателството за защита на данните*”. Поради тази причина администраторът трябва да избере доставчик на услуги в облака, който гарантира спазването на законодателството за защита на данните. Специален акцент трябва да се постави върху характеристиките на приложимите договори - те трябва да включват набор от стандартизирани гаранции за защита на личните данни, включително тези, очертани от РГ в параграф 3.4.3 (Технически и организационни мерки) и в параграф 3.5 (трансгранични потоци от данни) - както и допълнителни механизми, улесняващи комплексната проверка (due diligence) и отчетността (като например одити от независими трети страни и сертифициране на услугите на доставчика – вж. параграф 4.2).

Доставчиците на услуги в облака (обработващи лица) имат задължението да гарантират поверителността. Директива 95/46 ЕО гласи, че: „*Всяко лице, действащо под ръководството на администратора или на обработващия данни, включително самият*

[9] Фокусът на това становище е само върху стандартните отношения администратор-обработващ.

[10] Средата на изчислителните облаци може да се използва и от физически лица (потребители) за извършване само на лични или домашни дейности. В такъв случай трябва да се анализира внимателно, дали се прилага т.нар изключение за домакинство, което изключва потребителите от квалифицирането им като администратори. Този въпрос, обаче, е извън обхвата на това становище.

[11] Например Ниво на инструкции, наблюдение от клиента в облака, опит на страните

[12] Становище 1/2010 относно понятията „администратор на лични данни” и „лице, което обработва данните” - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

обработващ данни, и което има достъп до личните данни, може да ги обработва, само по указание на администратора, освен ако не е задължен да извърши това по закон". Достъпът до данни от страна на доставчика в изчислителния облак по време на предоставянето на услугите се ръководи изцяло от изискването за спазване на разпоредбите на чл. 17 от Директивата – вж. раздел 3.4.2.

Лицето, обработващо данните, трябва да вземе предвид вида на въпросния облак (публичен, частен, общностен или хибриден/IaaS, SaaS или PaaS [вж. Приложение а) Модели на проявление - б) Модели на доставка]) и вида на услугата, договорена с клиента. Обработващите носят отговорност за предприемане на мерки за сигурност, съответстващи на предвидените в законодателството на ЕС и прилагани в юрисдикциите на администратора и обработващия. Също така обработващите трябва да поддържат и подпомагат администраторите при спазване на (упражняването на) правата на субектите на данни.

3.3.2 Подизпълнители

В услугите в изчислителните облаци могат да са включени няколко договорни страни, които действат като лица, преработващи лични данни. Също така, обичайно е обработващите лица да възложат част от работата на допълнителни подизпълнители, които също получават достъп до личните данни. Ако обработващите възложат изпълнението на дадени услуги на подизпълнители, те са задължени да уведомят за това клиента, като му предоставят подробно описание на вида на възложената на подизпълнител услуга, характеристиките на настоящите или потенциални подизпълнители и гаранциите, че услугите, които те предлагат на доставчика на услуги в изчислителните облаци, са в съответствие с Директива 95/46/ЕО.

Всички съответни задължения трябва да се прилагат и към подизпълнителите на обработващия на базата на договори между доставчика на услуги в облака и подизпълнителя, отразяващи клаузите на договора между клиент и доставчик на услуги в облака. В своето Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните", Работната група по член 29 посочва многообразието на обработващите в случаите, в които те имат пряка връзка с администратора или да работят като подизпълнители, при което обработващите лица възлагат част от обработването, с което са били натоварени. „*Нищо в Директивата не пречи, поради организационни изисквания няколко субекта да бъдат посочени като лица, обработващи данните, или като техни подизпълнители чрез разпределяне на съответните задачи. Всички те, обаче, са длъжни да следват в процеса на обработването указанията, дадени от администратора на лични данни*."[13].

Произтичащите от законодателството за защита на данните задължения и отговорности трябва да са ясно посочени в тези варианти, а не да са разпръснати по цялата верига на възлагане или превъзлагане, с цел да се осигури ефективен контрол и ясно разпределяне на отговорността за обработването на данни.

Възможен модел на гаранции, които могат да се използват за уточняване на задълженията и отговорностите на лицата, обработващи лични данни, в случаите, когато те възлагат обработването на данните на подизпълнители, е въведен за първи път с решение на Европейската комисия от 5 февруари 2010 г. относно стандартните договорни клаузи за трансфер на лични данни на обработващи лица, установени в трети

[13] Вж. WP169, стр. 29, Становище 1/2010 относно понятията „администратор на лични данни" и „лице, което обработва данните" (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

страни[14]. В този модел превъзлагането е позволено само с предварителното писмено съгласие на администратора и с писмено споразумение, което налага на подизпълнителя същите задължения, наложени на лицето, обработващо личните данни. Когато подизпълнителят не успее да изпълни задълженията си за защита на данните съгласно такова писмено споразумение, обработващият остава изцяло отговорен пред администратора за изпълнението на задълженията на подизпълнителя съгласно това споразумение. Разпоредби от този вид могат да бъдат използвани в договорните клаузи между администратора и доставчика на услуги в изчислителния облак, при които последният възнамерява да предостави услуги чрез възлагане на подизпълнители, с цел да се осигурят необходимите гаранции за обработката на данни от подизпълнителите.

Подобно решение по отношение на гаранции в хода на обработката на данните от подизпълнители бе предложено неотдавна от Европейската комисия в нейното предложение за регламент за защита на данните[15]. Действията на обработващите трябва да се подчиняват на договор или друг законов акт, който обвързва обработващия данните с администратора и постановява, в частност, че наред с другите изисквания, обработващият трябва да включва други преработващи само с предварителното разрешение на администратора (чл. 26 (2) на предложението).

Съгласно мнението на РГ 29, обработващото лице може да възложи дейността си на подизпълнители само въз основа на съгласието на администратора, което обикновено се дава в началото на предоставянето на услугата[16] с ясното задължение за обработващия да информира администратора за всяко негово намерение за промени, включващи добавяне или замяна на подизпълнители, като администраторът си запазва правото по всяко време да се противопостави на такива промени или да прекрати договора. Доставчикът на услуги в облака трябва да има ясното задължение да посочва всички използвани подизпълнители. В допълнение, доставчикът на услуги в облака и подизпълнителят трябва да сключат договор, отразяващ разпоредбите на договора, сключен между клиента и доставчика на услуги в облака. Администраторът трябва да е в състояние да се възползва от договорното си право на възражение в случай на нарушаване на договора от страна на подизпълнителите. Това може да се уреди като се гарантира, че обработващият данните е пряко отговорен пред администратора за нарушенията, направени от неговите подизпълнители или чрез включването на клаузи за бенефициарни права на трети лица в полза на администратора в договорите, подписани между обработващия данните и подизпълнителя или чрез факта, че тези договори се подписват от името на администратора на лични данни, което го прави страна по договора.

3.4 Изисквания за защита на личните данни в отношенията клиент-доставчик

3.4.1 Съответствие с основните принципи

Законосъобразността на обработката на лични данни в облака зависи от спазването на основните принципи на законодателството на ЕС за защита на данни, а именно: да се гарантира прозрачност по отношение на субекта на данните, да се спазва принципа за определяне на целите и ограничаване на обработването на данните в рамките на тези цели, както и заличаване на личните данни, веднага след като тяхното задържане не е вече необходимо. Освен това, трябва да се въведат подходящи технически и

[14] Вж. Често задавани въпроси II.5 на WP176.

[15] Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица по отношение на обработката на личните им данни и свободното движение на тези данни, 25.01.2012 г.

[16] Вж. Често задавани въпроси II, 1) на WP176, прието на 12 юли 2010 г.

организационни мерки, за да се гарантира адекватно ниво на защита и сигурност на данните.

3.4.1.1 Прозрачност

Прозрачността е от ключово значение за справедливото и правомерно обработване на личните данни. Директива 95/46/ЕО задължава клиентите в облака да предоставят на съответното физическо лице, от което се събират данни, отнасящи се за него, информация за същността и целите на обработването на данни. Клиентът в облака трябва също така да предоставя всякаква допълнителна информация, като например информация за получателите или категориите получатели на данните, които могат да са обработващи лица и подизпълнители, доколкото тази допълнителна информация е необходима, за да се гарантира справедлива обработка на данните по отношение на техните субекти (вж. чл. 10 от директивата)[17].

Прозрачността трябва да е гарантирана и в отношението (отношенията) между клиента в облака, доставчика на услуги в облака и подизпълнителите (ако има такива). Клиентът в облака може да оцени законосъобразността на обработката на личните данни в облака, само ако доставчикът го информира за всички съответни въпроси. Администраторът, който възнамерява да ангажира доставчик на услуги в облака, трябва внимателно да провери процедурите и условията на доставчика на услуги в облака и да ги оцени от гледна точка на защитата на личните данни.

Прозрачността в облака означава, че клиентът в облака трябва да е информиран за всички подизпълнители, които участват в предоставянето на съответната услуга в облака, както и за местоположенията на всички центрове за данни, в които ще се обработват съответните лични данни.[18]

Ако предоставянето на услугата изисква инсталиране на софтуер в "cloud" системата на клиента (например, браузърни модули), доставчикът на услуги в облака като въпрос на добра практика следва да информира клиента за това обстоятелство и по-специално за последиците по отношение на защитата и сигурността на личните данни. Обратно, клиентът в облака трябва да повдигне този въпрос предварително, ако доставчикът на услуги в облака не му обърне достатъчно внимание.

3.4.1.2 Определяне на целта и ограничаване

Принципът на определяне на целта и ограничаване в нейните рамки налага изискването личните данни да се събират за конкретни, ясно формулирани и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели (вж. член 6(б) от Директива 95/46/ЕО). Клиентът на услуги в облака трябва да определи целта (целите) на обработката преди да пристъпи към събиране на лични данни от субектите и да ги информира за това. Клиентът в облака не бива да обработва личните данни за други цели, които не са съвместими с първоначалните.

Освен това, трябва да се гарантира, че личните данни не се обработват (незаконно) за други цели от доставчика на услуги в облака или някой от неговите подизпълнители. Тъй като типичният вариант на изчислителен облак може да включва по-голям брой

[17] Съответното задължение за информиране на субекта на данните е налице, когато се записват данни, които не са били получени от субекта на данни, а от различни източници или са разкрити от трети лица (вж. чл. 11).

[18] Само тогава той ще може да прецени, дали личните данни могат да бъдат прехвърлени към т. нар. трета страна извън Европейското икономическо пространство (ЕИП), която не гарантира адекватно ниво на защита по смисъла на Директива 95/46/ЕО. Вж. също т. 3.4.6 по-долу.

подизпълнители, рискът от обработването на лични данни за допълнителни и несъвместими цели трябва да се оцени като доста висок. За да се сведе до минимум този риск, договорът между доставчика на услуги в облака и клиента в облака трябва да включва технически и организационни мерки за намаляване на този риск и да предоставя гаранции за регистрация и проверка на съответните операции по обработване на личните данни, извършени от служители на доставчика на услуги в облака или на подизпълнителите.[19] Договорът трябва да предвижда наказания за доставчика или подизпълнителя в случай на нарушаване на законите за защита на личните данни.

3.4.1.3 Заличаване на данни

Съгласно чл.6(д) от Директива 95/46/ЕО, личните данни трябва да се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително. Личните данни, които не са необходими повече, трябва да се заличат или да се преобразуват в анонимни. Ако тези данни не могат да бъдат изтрити, поради правните норми за задържане (например, данъчни разпоредби), достъпът до тези лични данни трябва да се блокира. Клиентът в облака е отговорен да гарантира, че личните данни ще се заличат веднага, след като вече не са необходими в горепосочения смисъл[20].

Принципът на заличаване се прилага спрямо личните данни независимо от това, дали се съхраняват на твърди дискове или на други носители (напр. архивирани ленти). Тъй като личните данни, могат да се съхраняват дублирано на различни сървъри в различни места, трябва да се дадат гаранции, че всички носители са изтрити необратимо (т.е. трябва да се изтрият всички предишни версии, временни файлове и дори файлови фрагменти).

Клиентите в облака трябва да са наясно с факта, че данните за регистриране[21] на операциите за обработка на личните данни, напр. съхраняване, изменения или заличаване на данни, също могат да се квалифицират като лични данни, отнасящи се до лицето, което е инициирало съответната обработка.[22]

Сигурното изтриване на личните данни изисква унищожаване или размагнетизиране на носителите на данните или налага ефективното изтриване на съхранените данни чрез презаписване. За презаписване на личните данни трябва да се използват специални софтуерни инструменти, които да презапишат данните няколко пъти в съответствие с одобрена спецификация.

Клиентът в облака трябва да се увери, че доставчикът на услуги в облака гарантира сигурното изтриване в горепосочения смисъл, както и че договорът между доставчика и клиента съдържа ясни разпоредби за изтриване на личните данни[23]. Същото важи и за договорите между доставчиците и подизпълнителите в изчислителните облаци.

---

[19] Вж. раздел 3.4.3 по-долу.

[20] Изтриването на данните е въпрос, който е актуален през цялото времетраене на договора за предоставяне на услуги в изчислителни облаци и при неговото прекратяване. Той е от значение и в случай на заместване или оттегляне на подизпълнител.

[21] Забележките относно изискванията за регистриране са изложени по-долу в 4.3.4.2.

[22] Това означава, че трябва да се определят разумни срокове за задържане на файловете с регистрационни данни и да се въведат процедури, гарантиращи навременното заличаване или обезличаване на тези данни.

[23] Вж. раздел 3.4.3 по-долу.

3.4.2 Предпазни договорни клаузи в отношенията „администратор - обработващ лични данни”

Когато администраторите вземат решение за използване на услуги в изчислителни облаци, те са длъжни да изберат лице, обработващо данните, което осигурява достатъчни гаранции по отношение на мерките за техническа безопасност и организационните мерки, регулиращи обработването, което следва да се извърши и да осигури спазването на тези мерки (чл. 17(2) от Директива 95/46/ЕО). Освен това, те са законово задължени да подпишат официален договор с доставчик на услуги в облака, както е посочено в чл. 17(3) от Директива 95/46/ЕО. Този член налага изискването да се сключи договор или правен акт, който урежда отношенията между администратора и обработващия данните. За целите на съхраняване на доказателства, частите от договора или от правния акт, които се отнасят до защитата на данните, както и изискванията, свързани с техническите и организационните мерки, трябва да са в писмена или в друга равностойна форма.

Договорът трябва като минимум да осигурява условието, че обработващият данни действа само по указания на администратора и че обработващият трябва да прилага адекватни технически и организационни мерки за защита на личните данни.

За да се гарантира правната сигурност, договорът трябва да урежда следните въпроси:

1. Данни за (степента и условията на) указанията на клиента трябва да се предоставят на доставчика, по-специално по отношение на приложимите споразумения за нивото на услугите (които трябва да са обективни и измерими) и съответните санкции (финансови или други, включително възможността за подвеждане под съдебна отговорност на доставчика в случай на неизпълнение).
2. Уточняване на мерките за сигурност,които трябва да се вземат от доставчика на услуги в облака в зависимост от рисковете, свързани с обработването, и естеството на данните, които трябва да се защитят. От голямо значение е да се посочат конкретни технически и организационни мерки, като например тези, посочени в параграф 3.4.3 по-долу. Това не засяга прилагането на по-строги мерки, ако са приложими, които могат да се предвиждат съгласно националното законодателство на клиента.
3. Предмет и времева рамка на услугите в облака, които следва да се предоставят от доставчика на услуги в облака, степен, начин и цели на обработването на личните данни от страна на доставчика на услуги в облака, както и видове обработвани лични данни.
4. Уточняване на условията за връщане на (лични) данни или унищожаване на данните, след приключване на изпълнението на услугата. Освен това, трябва да се гарантира, че при искане на клиента на услуги в облака личните данни са заличени необратимо.
5. Включването на клауза за поверителност, която е задължителна за доставчика на услуги в облака и неговите служители, които имат достъп до данните. Само упълномощени лица могат да получат достъп до данните.
6. Задължение от страна на доставчика да оказва съдействие на клиента при упражняването на правата на субектите на данни за достъп, коригиране или изтриване на техните данни.
7. Договорът трябва изрично да определя изискването, че доставчикът на услуги в облака няма право да съобщава данни на трети страни, дори и за целите на опазване на данните, освен ако договорът не предвижда участието на подизпълнители. Договорът трябва да определя условието за ангажиране на

подизпълнители само при наличието на съгласие от администратора, заедно с ясното задължение обработващите данните да информират администратора за всяко свое намерение за въвеждането на промени в тази връзка, като администраторът си запазва правото по всяко време да се противопостави на такива промени или да прекрати договора. Доставчикът на услуги в облака трябва да има ясното задължение да обяви ангажираните подизпълнители (например, в публичен цифров регистър). Трябва да се гарантира, че договорите между доставчиците на услуги в изчислителните облаци и техните подизпълнители отразяват разпоредбите на договорите между клиентите и доставчиците на услуги в облака (т.е. че подизпълнителите са обект на същите договорни задължения, както и доставчиците на услуги в облака). В частност, трябва да се гарантира, че доставчиците на услуги в облака и подизпълнителите ще действат само по указанията на клиентите в облака. Както е обяснено в главата за подизпълнение, веригата на отговорност трябва да е ясно определена в договора. Обработващият данни трябва да има задължението да определя границите на международните трансфери, например чрез сключване на договори с подизпълнители на базата на стандартните договорни клаузи съгласно 2010/87/EU.

8. Изясняване на отговорността на доставчика на услуги в облака да уведоми клиента в случай на нарушаване на защитата на данните, което засяга данни на клиента в облака.
9. Задължение на доставчика на услуги в облак да предостави списък на местата, в които може да се осъществи обработването на данните.
10. Право на администратора да контролира, както и съответно задължение на доставчика на услуги в облака да оказва съдействие.
11. В договора трябва да се посочи, че доставчикът на услуги в облака трябва да информира клиента за съответните промени по отношение на конкретната услуга в облака, като например прилагането на допълнителни функции.
12. Договорът трябва да предвижда регистриране и проверка на съответните операции по обработване на лични данни, извършени от доставчика на услуги в облака или неговите подизпълнители.
13. Уведомяване на клиента в облака за всяко правно обвързващо искане от правоприлагащ орган за разкриване на лични данни, освен ако това не е забранено например по силата на наказателното право, с цел да се запази поверителността на разследването на правоприлагащите органи.
14. Общо задължение от страна на доставчика на услуги да гарантира, че вътрешната му организация на обработване на данни (както и тази на неговите подизпълнители, ако има такива) е в съответствие с приложимите национални и международни законови изисквания и стандарти.

В случай на нарушение от страна на администратора, лицата, претърпели вреди в резултат на незаконосъобразната обработка, трябва да имат право да получат обезщетение от администратора за причинените вреди. Ако лицата, обработващи данните, използват данните за каквато и да е друга цел или да ги разкрият или използват по начин, който нарушава договора, те също ще се считат за администратори и ще носят отговорност за нарушенията, в които са лично замесени.

В това отношение трябва да се отбележи, че в много случаи доставчиците на услуги в изчислителните облаци изготвят обикновено стандартни услуги и договори, които да бъдат подписани от администраторите на лични данни, с което де факто установяват стандартен начин за обработване на лични данни. Тази диспропорцията между

договорната сила на един дребен администратор на данни в сравнение с тази на доставчиците на услуги не трябва да се разглежда като оправдание за администратора да приема клаузи и договорни условия, които не са в съответствие със законодателството за защита на данните.

3.4.3 Технически и организационни мерки за защита на личните данни и гарантиране на сигурността на данните

Чл.17(2) от Директива 95/46/ЕО предвижда, че клиентите в облака (действащи като администратори на данни) са отговорни да изберат доставчици на услуги в облака, които прилагат необходимите технически и организационни мерки за сигурност и защита на личните данни, както и да са в състояние да докажат изпълнението на това условие.

В допълнение към основните цели за осигуряване на достъпността, поверителността и достоверността на данните, трябва да се обърне внимание и на допълнителните цели за защита на данните, включващи прозрачност (вж. 3.4.1.1 по-горе), изолация[24], възможност за интервенция, отчетност и преносимост. Този раздел разглежда тези централни цели за защита на данните, без да засяга анализа на риска, ориентиран към другите допълнителни мерки за сигурност[25].

3.4.3.1 Достъпност

Осигуряването на достъпност означава гарантиране на навременен и надежден достъп до личните данни.

Сериозна заплаха за достъпността на данните в облака е случайната загуба на мрежова връзка между клиента и доставчика или на прекъсване на работата на сървъра, причинено от злонамерени действия, като например (разпространена) атака за отказ на услуга (DoS)[26]. Другите рискове за достъпността включват случайни хардуерни повреди, както в мрежата, така и в системите за обработка и съхранение на данни в облака, електрически аварии и други проблеми с инфраструктурата.

Администраторите на данни трябва да проверят, дали доставчикът на услуги в облака е предприел разумни мерки за избягване на риска от прекъсвания, като например архивиране на линкове към интернет мрежата, резервирано съхранение и ефективни механизми за архивиране на данни.

3.4.3.2 Цялост

Целостта може да се дефинира като свойството на автентичност на данните, което дава гаранция, че данните не са променени злонамерено или случайно по време на обработването, съхранението или прехвърлянето. Понятието достоверност може да се разшири в информационните системи и да наложи изискването при обработването на лични данни в тези системи, те да останат непроменени.

---

[24] В Германия в законодателството е въведено по-широкото понятие "несвързаност", което е прието от Конференцията на комисионерите по защита на личните данни.

[25] Вж. напр. Европейска мрежа и агенция за информационна сигурност (ENISA) на http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment

[26] Атаката за отказ на услуга (DoS) е координиран опит временно или за неопределено време да се направи конкретен компютър или мрежов ресурс недостъпен за оторизираните потребители (например, с помощта на голям брой атакуващи системи, които парализират целта с множество външни искания за комуникация).

Установяването на промени в личните данни може да се постигне чрез криптографски механизми за автентификация, като например кодове за идентификация на съобщението или подписите.

Нарушаването на достоверността на информационните системи в облака може да се предотврати или открие със средствата за откриване на проникване/системи за превенция (IPS/IDS). Това е особено важно при отворените мрежови среди, в които обикновено работят изчислителните облаци.

3.4.3.3 Поверителност

В изчислителния облак шифрирането може да допринесе значително за гарантиране на поверителността на личните данни, ако се прилага правилно, въпреки че не прави личните данни необратимо анонимни[27]. Шифрирането на личните данни трябва да се използва във всички случаи на „транзитни" данни и когато е възможно при данните „в покой".[28] В някои случаи (например, услугата за съхранение IaaS) клиентът в облака може да не разчита на решение за шифриране, предложено от доставчика на услуги в облака, а да избере шифриране на личните данни преди тяхното изпращане в облака. Шифроването на данните в покой изисква особено внимание към управлението на криптографските ключове, тъй като сигурността на данните в крайна сметка зависи от поверителността на шифроващите ключове.

Комуникацията между доставчика на услуги и клиента в облака, както и между центровете за данни трябва да е кодирана. Дистанционното администриране на платформата на облака трябва да се осъществява само чрез сигурен канал за комуникация. Ако клиент планира не само да съхранява, но също така и допълнително да обработва личните данни на облака (например, търсене на справки в бази от данни), той трябва да има предвид, че шифрирането не може да се поддържа по време на обработването на данните (с изключение на някои много специфични изчисления).

Допълнителните технически мерки, насочени към осигуряване на поверителност, включват механизми за разрешаване и силна автентификация (напр. двуфакторна автентификация). Договорните клаузи също трябва да налагат задължения за поверителност на служителите на клиентите в облака, доставчиците на услуги в облака и техните подизпълнители.

3.4.3.4 Прозрачност

Техническите и организационните мерки трябва да гарантират прозрачност, която позволява извършването на прегледи, вж. 3.4.1.1.

3.4.3.5 Изолиране (ограничаване на целта)

В инфраструктурите на изчислителните облаци между много ползватели се споделят различни ресурси, като например памет и мрежи. Това създава нови рискове, включващи оповестяване и обработване на данните за неправомерни цели. Целта на

[27] Директива 95/46/ЕО - Съображение 26: „(...) като имат предвид, че принципите на защита не се отнасят до данни, които са направени анонимни по начин, който прави невъзможно идентифицирането на съответното физическо лице (...)". В същия смисъл, техническите процеси за раздробяване на данни, които могат да бъдат използвани в рамките на предоставянето на услуги в изчислителните облаци, не водят до необратима анонимност и следователно това не означава, че задължението за защита на данните не се отнася за този случай.

[28] Това важи по-специално за администраторите на лични данни, които планират да прехвърлят чувствителни данни по смисъла на чл.8 от Директива 95/46/ЕО (например, здравни данни) в системата на изчислителен облак или които са предмет на конкретни правни задължения за професионална тайна.

предпазното „изолиране" е да се занимае с този въпрос и да осигури гаранции, че данните не се използват извън първоначалната цел на тяхното обработване (чл.6(б) от Директива 95/46/ЕО) и да се поддържа тяхната поверителност и достоверност.[29]

Постигането на изолирането на първо място изисква адекватно управление на правата и ролите за достъп до лични данни, които следва да се преразглеждат редовно. Трябва да се избягва определянето на роли с прекомерни привилегии (например, никой от потребителите или администраторите не бива да има разрешен достъп до целия облак). По-общо казано, администраторите и потребителите трябва да имат достъп само до информацията, която е необходима за изпълнението на техните законни цели (принципът на най-малка привилегия).

На второ място, изолацията също така зависи от предприетите технически мерки, като например подсилване на софтуера за управление и правилното управление на споделените ресурси, ако се използват виртуални машини за споделяне на физически ресурси между различните клиенти в облака.

3.4.3.5 Възможност за намеса

Директива 95/46/ЕО дава на субектите на данни правото на достъп, поправка, заличаване, блокиране и възражение (вж. чл.12 и 14). Клиентите в облака трябва да се уверят, че доставчиците на услуги в облака не налагат технически и организационни пречки пред тези изисквания, включително и в случаите, когато данните се обработват допълнително от подизпълнители.

Договорът между клиента и доставчика трябва да предвижда условието, че доставчикът на услуги в облака е длъжен да съдейства на клиента за улесняване на упражняването на правата на субектите на данни и да гарантира, че същото важи и по отношение на неговите подизпълнители.[30]

3.4.3.6 Преносимост

Понастоящем, повечето доставчици на услуги в облака не използват стандартни формати за данни и обслужващи интерфейси за улесняване на оперативната съвместимост и преносимост между различни доставчици на услуги в изчислителните облаци. Ако даден клиент в облака вземе решение да се прехвърли от един доставчик на услуги в облака към друг, липсата на оперативна съвместимост може да доведе до невъзможност или най-малкото до затруднения при прехвърлянето на (личните) данни на клиента към новия доставчик на услуги в облак (т. нар. зависимост на клиента от доставчика на услуги). Същото важи и за услугите, които клиентът е разработил върху платформа, предоставена от първоначалния доставчик на услуги в облака (PaaS). Клиентът в облака трябва да провери дали и как доставчикът гарантира преносимостта на данните и услугите, преди да се ангажира с поръчка на услуги в облака.[31]

3.4.4.7 Отчетност

В информационните технологии отчетността може да се определи като способността да се установи какво е направило дадена структура в определен момент в миналото и как.

---

[29] Вж. 3.4.1.2.

[30] Вж. раздел 3.4.5 № 7 по-горе. Доставчикът може дори да е инструктиран да отговаря на исканията от името на клиента.

[31] За предпочитане е доставчикът на услуги да използва стандартизирани или отворени формати за данни и интерфейси. Във всеки случай следва да се договорят клаузи, предвиждащи сигурни формати, запазване на логическите връзки и всички разходи, произтичащи от миграцията към друг доставчик на услуги в облака.

В областта на защитата на личните данни отчетността често има по-широк смисъл и описва способността на страните да докажат, че са предприели необходимите стъпки, за да се гарантира, че са спазени принципите на защита на данните.

Отчетността в информационните технологии е особено важна при разследване на нарушенията на сигурността на личните данни, при които клиентите в облака, доставчиците на услуги и техните подизпълнители могат да имат определена степен на оперативна отговорност. Способността на платформата в облака да осигури надежден мониторинг и цялостни механизми за регистриране е от първостепенно значение в това отношение.

Освен това, доставчиците на услуги в облака следва да предоставят писмени доказателства за подходящи и ефективни мерки, които осигуряват прилагането на принципите за защита на личните данни, описани в предходните раздели. Примери за такива мерки са процедурите за идентификация на всички операции за обработване на данни, отговорите на исканията за достъп, разпределението на ресурсите, включително определянето на служители по защита на личните данни, отговорни за организацията на съответствието на защитата на данните или независимите процедури за сертифициране. В допълнение, администраторите на лични данни трябва да гарантират, че имат готовност да демонстрират установяването на необходимите мерки пред компетентните надзорни органи при поискване.[32]

3.5 Международни трансфери

Чл.25 и чл.26 от Директива 95/46/ЕО разглеждат свободния поток на лични данни към страни, разположени извън ЕИП, само ако тази страна или получатели гарантират адекватно ниво на защита на данните. В противен случай трябва да се въведат специфични предпазни мерки от администратора и другите съ-администратори и/или лицето, обработващо личните данни. Въпреки това, изчислителните облаци най-често се основават на пълна липса на стабилно местоположение на данните в мрежата на доставчика на услуги в облака. Данните могат да са в един център за данни в 14:00 ч. и в друга част на света в 16:00 ч. Затова клиентът в облака рядко може да е сигурен за реалното време, в което данните са разположени, запазени или прехвърлени. В този контекст съществуват ограничения на традиционните правни инструменти за осигуряване на рамка за регулиране на трансфера на данни в трети страни извън страните-членки на ЕС, които не осигуряват адекватна защита.

3.5.1 Safe Harbour и адекватност на страните

Констатациите за адекватност, включително личната неприкосновеност, са ограничени по отношение на географския обхват и следователно не включват всички трансфери в рамките на изчислителния облак.
Съгласно законодателството на ЕС могат да се осъществяват законни трансфери към американски организации, които се придържат към принципите, тъй като се счита, че организациите-получатели осигуряват адекватно ниво на защита на предаваните данни.

Въпреки това, Работната група е на мнение, че само самостоятелното сертифициране за лична неприкосновеност (Safe Harbor) не може да се счита за достатъчно при липсата на устойчиво прилагане на принципите за защита на данните в средата на изчислителните облаци. В допълнение, за целите на обработването на личните данни чл.17 от Директивата на ЕС изисква подписването на договор между администратора

[32] Работната група предостави подробни бележки относно отчетността в своето Становище 3/2010 относно принципа на отчетност http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

на данни и обработващия, което се потвърждава в отговора на въпрос 10 (FAQ) на рамковите документите за гарантиране на личната неприкосновеност, подписани между ЕС и САЩ. Този договор не подлежи на предварително одобрение от страна на европейските органи за защита на данните. Той определя обработването, което следва да се извърши, както и всички мерки, необходими да се гарантира сигурността на съхраняване на данните. Различните национални законодателства и органи за защита на личните данните могат да имат допълнителни изисквания.

Работната група смята, че компаниите, експортиращи лични данни, не бива да разчитат само на изявлението на вносителя на данни, потвърждаващо че той е сертифициран за осигуряване на личната неприкосновеност. Напротив, компанията, която експортира данните, трябва да получи доказателства, че са налице самостоятелни сертификации за лична неприкосновеност, както и да поиска доказателства, доказващи спазването на принципите на такива сертификации. Това е особено важно по отношение на информацията, предоставена на субектите на данни, които са засегнати от обработването на личните данни[33,34].

Работната група също така счита, че клиентът в облака трябва да провери, дали стандартните договори, съставени от доставчиците на услуги в облака, са в съответствие с националните изисквания по отношение на договореното обработване на лични данни. Националното законодателство може да изисква възлагането на обработването на данни на подизпълнители да бъде дефинирано в договора, който включва местоположението и други данни за подизпълнителя, както и проследяването на данните. Обикновено доставчиците на услуги в облака не предоставят на клиента такава информация – техният ангажимент за лична неприкосновеност замества липсата на горните гаранции, когато това се изисква от националното законодателство. В такива случаи на износителя се препоръчва да използва други правни инструменти, като например стандартните договорни клаузи или задължителни корпоративни правила.

И накрая, Работната група смята, че принципите на лична неприкосновеност сами по себе си също не могат да осигурят необходимите средства на износителя на данни, за да се гарантира, че доставчикът на услуги в облака, установен в САЩ, използва подходящи мерки за сигурност, които може да се изискват от националните законодателства на базата на Директива 95/46/ЕО[35]. По отношение на сигурността на данните, изчислителните облаци пораждат няколко вида рискове, които са специфични за операциите в облака, като например загуба на управление, несигурно или непълно заличаване на данни, недостатъчно одитно проследяване или невъзможност за изолация[36], които не са включени в достатъчна степен в съществуващите принципи на лична неприкосновеност по отношение на сигурността на данните[37]. По този начин могат да се въведат допълнителни гаранции за сигурността на данните, например чрез

[33] Вж. Германския орган за защита на личните данни: http://www.datenschutzberlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] За изискванията по отношение на подизпълнителите, обработващи данни, вж. 3.3.2.

[35] Вж. също и становището на датския орган за защита на личните данни: http://www.datatilsynet.dk/english/processing-of-sensitive-personaldata-in-a-cloud-solution.

[36] Подробности са дадени в документа на Европейската мрежа и агенция за информационна сигурност (ENISA) относно изчислителните облаци: Ползи, рискове и препоръки за информационната сигурност, представени на адрес: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment.

[37] „Организацията трябва да вземе разумни предпазни мерки, за да защити личните данни срещу загуба, неправомерно използване и неразрешен достъп, разкриване, промяна и разрушаване."

включване на опита и ресурсите на трети лица, които са в състояние да направят оценка на адекватността на доставчиците на услуги в облака чрез различни схеми на проверка, стандартизация и сертифициране[38]. Поради тези причини е разумно да се допълни задължението на вносителя на данни за осигуряване на личната неприкосновеност с допълнителни предпазни мерки, като се вземе предвид специфичния характер на облака.

3.5.2 Изключения

Изключенията, предвидени в чл.26 от Директивата на ЕС 95/46/ЕО дават възможност на износителите на данни да прехвърлят данни от ЕС, без да предоставят допълнителни гаранции. Въпреки това, РГ по чл. 29 е приела становище, в което тя счита, че могат да се прилагат изключения, само когато прехвърляните данни не са повтарящи се, масивни или структурирани.[39]

Въз основа на тези интерпретации е почти невъзможно да се разчита на изключения в контекста на изчислителните облаци.

3.5.3 Стандартни договорни клаузи

Стандартните договорни клаузи, приети от Европейската комисия за целите на рамкиране на международните трансфери на данни между два администратора на данни или между един администратор на данни и едно лице, обработващо тези данни се основава на двустранен подход. Когато доставчикът на услуги в облака се счита за обработващ данните, стандартните клаузи съгласно Решение 2010/87/ЕС са инструментът, който може да се използва от администратора на данни и обработващия данните като база за гарантиране, че изчислителният облак предлага достатъчни гаранции в контекста на международните трансфери.

В допълнение към стандартните договорни клаузи, Работната група смята, че доставчиците на услуги в облака могат да предложат на клиентите разпоредби, изградени на базата на прагматичния им опит, доколкото те не противоречат пряко или косвено на стандартните договорни клаузи, одобрени от ЕК, или доколкото те не накърняват основните права или свободи на субектите на данни[40]. Компаниите, обаче, не могат да допълват или променят стандартните договорни клаузи, без това да доведе до предположението, че клаузите вече не са „стандартни”[41].

Когато доставчикът на услуги в облака, действащ в качеството си на обработващ личните данни, е установен в ЕС, ситуацията може да се окаже по-сложна, тъй като по принцип примерните клаузи се прилагат само за прехвърлянето на данни от администратор в рамките на ЕС към лице, обработващо данните извън ЕС (вж. съображение 23 на решението на Комисията за примерните клаузи 2010/87/EU и WP176).

---

[38] Вж. раздел 4.2 по-долу.

[39] Работен документ 12/1998 г.: Трансфер на лични данни към трети страни: прилагане на членове 25 и 26 от директивата на ЕС за защита на личните данни, приет от Работната група на 24 юли 1998 г. (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

[40] Вижте Често задавани въпроси (FAQ) IV B1.9 9, Могат ли компаниите да включват стандартни договорни клаузи в договори с по-широк обхват и да добавят специфични клаузи?, публикуван от ЕК на адрес:
http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[41] Вижте Често задавани въпроси (FAQ) IV B1.10, Могат ли компаниите да изменят и променят стандартните договорни клаузи, одобрени от Комисията?

По отношение на договорните отношения между лицето, което обработва данните извън ЕС и съответните подизпълнители трябва да е налице писмено споразумение, което налага същите задължения на подизпълнителя, каквито са наложени на обработващия данните в примерните клаузи.

3.5.4 Задължителни корпоративни правила: развитие към глобален подход

Задължителните корпоративни правила (BCR) представляват кодекс на поведение на компаниите, които осъществяват прехвърляне на данни в рамките на своята група. Такова решение се предвижда и в контекста на изчислителните облаци, когато доставчикът обработва лични данни. Всъщност в момента РГ29 работи по определяне на задължителните корпоративни правила за лицата, обработващи лични данни, което ще позволи прехвърлянето в рамките на групата в полза на администраторите без да е необходимо подписването на договори между обработващия данните и неговите подизпълнители за всеки клиент.[42]

Наличието на такива задължителни корпоративни правила за лицата, обработващи лични данни, ще даде възможност на клиента на доставчика на услуги в облака да предоставя своите лични данни на обработващото лице, като в същото време получава гаранции, че данните, прехвърлени в рамките на обхвата на дейността на доставчика, ще получат адекватно ниво на защита.

4. Заключения и препоръки

Фирмите и администрациите, които възнамеряват да използват изчислителни облаци, като първа стъпка трябва да извършат цялостен и задълбочен анализ на риска. Този анализ трябва да включва рисковете, свързани с обработката на данни в изчислителния облак (липса на контрол и недостатъчна информация – вж. раздел 2 по-горе), като се вземе предвид типа данни, обработвани в облака.[43] Трябва да се обърне специално внимание на оценката на правните рискове по отношение на защитата на данните, които се отнасят главно за задълженията за осигуряване на сигурност на данните и международни прехвърляния на данни. Обработването на чувствителни данни чрез изчислителни облаци поражда допълнителни опасения. Следователно, без да се засягат националните закони, обработването изисква допълнителни предпазни мерки.[44] Заключенията по-долу са предназначени да осигурят списък за проверка за спазването на изискванията за защитата на данните от клиентите и доставчиците на услуги в изчислителните облаци на базата на действащата правна рамка; представени са и някои препоръки с оглед на бъдещите промени в регулаторната рамка на ниво ЕС и извън него.

4.1 Насоки за клиентите и доставчиците на услуги в изчислителните облаци

– Връзка между администратора на лични данни и лицето, обработващо тези данни: Това становище се фокусира върху отношенията клиент-доставчик като отношение между администратор-обработващ лични данни (вж. параграф

[42] Вж. Работен документ 02/2012, който определя таблица с елементи и принципи, които могат да бъдат включени в Задължителните корпоративни правила на лицето, обработващо данните, приет на 6 юни 2012 г.: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[43] Европейската мрежа и агенция за информационна сигурност (ENISA) предоставя списък на рисковете, които трябва да се вземат под внимание http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[44] Вж. Сопотския меморандум, вж. бележка 2 по-горе.

3.3.1); въпреки това, на базата на конкретните обстоятелства могат да съществуват ситуации, в които доставчикът на услуги в облака действа и в качеството си на администратор, например, когато доставчикът на услуги преработва личните данни за свои собствени цели. В такъв случай доставчикът на услуги в облака носи пълната (съвместна) отговорност за обработката на данни и трябва да изпълнява всички задължения, предвидени от Директиви 95/46/ЕО и 2002/58/ЕО (ако е приложимо);

- Отговорността на клиента в облака като администратор на данни: Клиентът, в качеството си на администратор на данни е длъжен да поеме отговорността за съблюдаването на законодателството за защита на личните данни и за него се отнасят всички правни задължения, посочени в Директива 95/46/ЕО и Директива 2002/58/ЕО, когато са приложими, по-специално по отношение на субектите на данни (вж. 3.3.1). Клиентът трябва да избере такъв доставчик на услуги в облака, който гарантира спазването на законодателството на ЕС за защита на личните данни, както е отразено в съответните договорни гаранции, обобщени по-долу;
- Гаранции при наличие на подизпълнители: Всеки договор между доставчиците на услуги в изчислителния облак и клиентите в облака трябва да включа клаузи за подизпълнителите. Договорът трябва да уточнява, че обработването на данни може да се възлага на подизпълнители само въз основа на общото съгласие на администратора на данни с ясното задължение за обработващия да информира администратора на данни за всяко свое намерение за промени в това отношение, като администраторът си запазва правото по всяко време да се противопостави на такива промени или да прекрати договора. Доставчикът на услуги в облака трябва да има ясното задължение да посочи всички използвани подизпълнители. Доставчикът на услуги в облака трябва да сключи договор с всички ангажирани от него подизпълнители, който следва да отразява разпоредбите на договора, сключен с клиента в облака; клиентът трябва да се увери, че разполага с договорни възможности в случай на нарушаване на договора от страна на подизпълнителите на доставчика (вж. 3.3.2);
- Спазване на основните принципи на защита на личните данни:
  - Прозрачност (вж. 3.4.1.1): доставчиците на услуги в облака трябва да информират клиентите в облака за всички (свързани със защитата на данните) съответни аспекти на услугите си по време на преговорите по договора; по-конкретно, клиентите трябва да са информирани за всички подизпълнители, които допринасят за изпълнението на съответната услуга в изчислителния облак и за всички места, на които данните могат да бъдат съхранявани или обработвани от доставчика на услуги в облака и/или от неговите подизпълнители (особено, ако някои или всички места са извън Европейското икономическо пространство (ЕИП)); клиентът трябва да разполага със значима информация за техническите и организационните мерки, прилагани от доставчика; като въпрос на добра практика клиентът следва да информира субектите на данни за доставчика на услуги в облака и за всички подизпълнители (ако има такива), както и за местата, на които данните могат да бъдат съхранявани или обработвани от доставчика на услуги в облака и/или неговите подизпълнители;
  - Определяне на целта и ограничаване на обработването в нейните рамки (3.4.1.2): Клиентът трябва да гарантира спазването на принципите за определяне на целта и ограничаване на обработването на данни в нейните рамки, като гарантира, че данните няма да се обработват за други цели от доставчика на услуги или от неговите подизпълнители. Ангажиментите в

тази насока трябва да са потвърдени в съответните договорни мерки (включително техническите и организационните предпазни мерки);

- Задържане на данните (3.4.1.3): Клиентът е задължен да гарантира, че личните данни се изтриват (от доставчика и всички подизпълнители) от мястото, където се съхраняват, веднага, след като вече не са необходими за постигането на конкретните цели; договорът следва да предостави сигурни механизми за изтриване (унищожаване, размагнетизиране, презаписване);

– Договорни предпазни клаузи (вж. 3.4.2, 3.4.3 и 3.5):
  - Общи: договорът с доставчика (както и договорите, сключени между доставчика и подизпълнителите) трябва да дава достатъчно гаранции по отношение на техническата сигурност и организационните мерки (съгласно чл.17(2) от директивата) и трябва да е изготвен в писмена или друга равностойна форма. Договорът трябва да включва подробни указания, изготвени от клиента и предназначени за доставчика, включващи предмета и времевата рамка на услугите, целите и измеримите нива на обслужване и съответните санкции (финансови или други); той трябва да посочи мерките за сигурност, които следва да бъдат спазвани като функция на рисковете от обработването и естеството на личните данни в съответствие с посочените по-долу изисквания, както и да са предмет на по-строги мерки, като тези, предвидени в националното законодателство на клиента; ако доставчиците на услуги в облака възнамеряват да използват стандартни договорни условия, те трябва да гарантират, че тези условия са в съответствие с изискванията за защита на данните (вж. 3.4.2), най-вече техническите и организационните мерки, предприети от доставчика, трябва да се уточнят в съответните условия;
  - Достъп до данните: Само упълномощени лица трябва да имат достъп до данните; договорът трябва да съдържа клауза за поверителност по отношение на доставчика на услуги и неговите служители;
  - Разкриване на данни на трети страни: този въпрос следва да се регулира само чрез договор, който включва задължение за доставчика да назове всички свои подизпълнители - например в публичен цифров регистър - и да осигури на клиента достъп до информацията за всички промени, за да може клиентът евентуално да се противопостави на тези промени или да прекрати договора; договорът следва да изисква от доставчика да уведомява клиента за всяко правно обвързващо искане за разкриване на лични данни от страна на правоприлагащите органи, освен ако такова оповестяване е забранено поради други причини; клиентът трябва да има гаранция, че доставчикът ще отхвърли всички незаконосъобразни задължителни искания за разкриване на информация;
  - Задължения за оказване на съдействие: клиентът трябва да има гаранция, че доставчикът е длъжен да му съдейства по отношение на правото на клиента да контролира операциите, свързани с обработването на данни, да улесни упражняването на правата на субектите на данни за достъп/коригиране/изтриване на техните данни и (когато това е приложимо) да уведоми клиента в облака за всички нарушения, засягащи данните на клиента;
  - Трансгранично прехвърляне на данни: клиентът в облака трябва да провери, дали доставчикът на услуги в облака може да гарантира законността на трансграничното прехвърляне на данни и ако е възможно, да ограничи прехвърлянето само до страни, одобрени от клиента. Прехвърлянето на

данни в неодобрени трети страни изисква специфични предпазни мерки, включващи използването на договорености по Safe Harbor, стандартни договорни клаузи (СДК) или обвързващи корпоративни правила (ОКП), според конкретния случай; използването на СДК за лицата, обработващи лични данни (съгласно Решение на Европейската комисия 2010/87/ЕО), изисква определена адаптация към средата на изчислителните облаци (за да се предотврати сключването на отделни договори за всеки един клиент между доставчика на услуги и неговите подизпълнители), която предполага необходимостта от предварително получаване на разрешение от компетентния орган за защита на личните данни; договорът трябва да включва списък на местата, в които могат да бъдат предоставяни данните;

- Регистриране и проверка на обработването на данни: клиентът трябва да поиска регистриране на операциите по обработване на данните, извършвани от доставчика и неговите подизпълнители; клиентът трябва да бъде упълномощен да извършва проверки на тези операции по обработване на данни, като в същото време е допустимо извършването на проверки и сертифициране от трети страни, избрани от администратора на лични данни при условие, че е осигурена пълна прозрачност (например чрез предоставяне на възможност за получаване на копие от проверките на тези трети страни, сертификатите или копия на одиторските доклади, потвърждаващи сертифицирането);
- Технически и организационни мерки: те трябва да бъдат насочени към преодоляване на рисковете, произтичащи от липсата на контрол и липсата на информация, които се проявяват най-вече в средата на изчислителните облаци. Първите мерки са насочени към осигуряване на достъпност, достоверност, поверителност, изолация, възможност за намеса и преносимост на данните, както е определено в документа, а последните мерки акцентират върху прозрачността (вж. 3.4.3 за повече информация).

4.2 Сертифициране на защитата на личните данни от трета страна

- Независимата проверка или сертифицирането от реномирана трета страна може да е надеждно средство, с което доставчиците на услуги в облака могат да докажат, че спазват задълженията си, посочени в настоящото становище. Като минимум, такова сертифициране показва, че мерките за контрол на защитата на личните данни са били обект на проверка или преглед на базата на признат стандарт, отговарящ на изискванията, посочени в настоящото становище от страна на реномирана организация.[45] В контекста на изчислителните облаци, потенциалните клиенти трябва да преценят, дали доставчиците на услуги в изчислителния облак могат да предоставят копие от такъв сертификат за проверка от трета страна или копие на одиторския доклад, потвърждаващ сертифицирането, включващ изискванията, изложени в настоящото становище.
- Извършването на индивидуални проверки на данните, поместени в многостранна, виртуална сървърна среда, може да се окаже непрактично от техническа гледна точка и в някои случаи може да увеличи рисковете за въведените контролни мерки за физическа и логическа сигурност в мрежата. В такива случаи проверката, извършена от трета страна, избрана от

[45] Тези стандарти включват документите, издадени от Международната организация по стандартизация, Съвета за международни стандарти за одит и гаранции и Съвета за одиторски стандарти на Американския институт на дипломираните експерт-счетоводители дотолкова, доколкото тези организации издават стандарти, които отговарят на изискванията, посочени в настоящото становище.

администратора на данни, може да се счита за достатъчна, вместо извършването на индивидуални проверки, на които администраторът на данни има право.

- Приемането на конкретни стандарти и сертификати, свързани с неприкосновеността на личния живот, е от основно значение за създаването на надеждна връзка между доставчиците на услуги в облака, администраторите на данни и субектите на тези данни.
- Тези стандарти и сертификати трябва да са насочени към техническите мерки (като например локализиране на данни или шифриране), както и към процесите в рамките на организацията на доставчиците на услуги в облака, които гарантират защита на данните (като например политики за контрол на достъпа, мерки за контрол на достъпа или архивиране).

4.3 Препоръки: бъдещо развитие

Работната група е напълно наясно, че сложността на изчислителните облаци не може да се обхване напълно чрез използването на предпазните мерки и решения, очертани в настоящото становище, но те все пак осигуряват стабилна основа за защита на обработването на личните данни, които клиенти, установени в ЕИП, възлагат на доставчици на услуги в изчислителните облаци. Този раздел има за цел да подчертае някои проблеми, които трябва да бъдат решени в краткосрочен и средносрочен план, за да се подсилят въведените предпазни мерки с цел да се окаже съдействие на икономическата дейност в изчислителните облаци по отношение повдигнатите въпроси, като същевременно да се гарантира зачитането на основните права на защита на личния живот и личните данни.

– По-добро балансиране на отговорностите между администратора на лични данни и лицето, обработващо данните: Работната група приветства разпоредбите, съдържащи се в чл.26 на предложенията на ЕК (Проект на ЕС за Общ регламент за защита на данните), целта на които е да повишат нивото на отчетност на лицата, обработващи личните данни, пред администраторите на тези данни, като им съдействат при осигуряването на съответствие, по-специално по отношение на задълженията за сигурност и другите свързани задължения. Чл.30 от предложението въвежда правно задължение за лицето, обработващо лични данни, да прилага подходящи технически и организационни мерки. Проектите на предложенията изясняват, че обработващият лични данни, който не спазва указанията на администратора на данни, следва да се квалифицира като администратор на данни и подлежи на валидни конкретни съвместни правила за контрол. Работната група по чл.29 счита, че това предложение е в правилната посока за преодоляване на несъответствието, което често се среща в средата на изчислителните облаци, при което клиентът (особено ако е малко или средно предприятие) среща затруднения при упражняването на необходимия контрол, изискван от законодателството за защита на личните данни, върху начина, по който доставчикът предоставя исканите услуги. Освен това, с оглед на асиметричното правно положение на субектите на данни и малките бизнес потребители спрямо големите доставчици на услуги в изчислителните облаци, се препоръчва по-активна роля на организациите за защита на потребителите и бизнес интересите с цел да се договорят по-балансирани общи условия на договорите с такива компании.

– Достъп до лични данни за целите на националната сигурност и правоприлагането: от първостепенно значение е бъдещият регламент да се допълни с изискването за забрана на администраторите на данни, работещи в ЕС, да разкриват лични данни на трета страна, ако това е наредено от съдебните или административните органи на

тази трета страна, освен ако това не е изрично разрешено по силата на международно споразумение или договори за правна взаимопомощ или одобрено от надзорния орган. Регламент (ЕО) № 2271/96 е подходящ пример за такова правно основание.[46] Работната група е загрижена за тази липса в предложението на Комисията, тъй като тя води до значителна загуба на правна сигурност за субектите на данни, чиито лични данни се съхраняват в центрове за данни по целия свят. Поради тази причина, Работната група би искала да подчертае[47] необходимостта да се допълни регламента със задължението за използване на договори за правна взаимопомощ (MLAT) в случай на оповестявания, които не са разрешени от законодателството на Европейския съюз или държавите-членки.

– Специални предпазни мерки от страна на публичния сектор: Трябва да се добави специално условие за необходимостта дадена публична институция първо да направи оценка, дали съобщаването, обработването и съхранението на данни извън националната територия може да изложи на неприемлив риск сигурността и неприкосновеността на личния живот на гражданите и националната сигурност и икономика - по-специално, ако са засегнати чувствителни бази от данни (например данни от преброяване) и услуги (например здравеопазване)[48]. Такова специално внимание трябва да се обръща във всички случаи, когато се обработват чувствителни данни в изчислителните облаци. От тази гледна точка националните правителства и европейските институции на Съюза трябва да обмислят продължаването на проучването на идеята на европейски правителствен изчислителен облак като над национално виртуално пространство, в което може да се прилага последователен и хармонизиран набор от правила.

– Европейско облачно партньорство: Работната група подкрепя стратегията за Европейско облачно партньорство (ЕОП), представена от г-жа Крус, заместник председател на Европейската комисия, през януари 2012 г. в Давос.[49] Тази стратегия включва обществени поръчки в областта на информационните технологии, които ще стимулират европейския пазар за облачни услуги. Прехвърлянето на лични данни в европейски доставчик на услуги в изчислителните облаци, подчиняващ се на разпоредбите на европейското законодателство за защита на личните данни, може да донесе големи предимства за клиентите по отношение на защитата на личните данни, най-вече чрез насърчаване на приемането на общи стандарти (особено по отношение на оперативната съвместимост и преносимост на данните), както и по отношение на правната сигурност.

---

[46] Регламент (ЕО) № 2271/96 на Съвета от 22 ноември 1996 г. относно защитата срещу последиците от извънтериториалното прилагане на законодателство, прието от трета страна, и действията, предприети на основание това законодателство или произтичащи от него, Официален вестник L 309 , 29/11/1996 P. 0001 - 0006, URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML

[47] Вж. WP191 - Становище 01/2012 г. относно предложенията за реформи за защита на данните, стр. 23.

[48] В това отношение ENISA прави следната препоръка в документа си за сигурност и устойчивост в правителствените изчислителни облаци (http://www.enisa.europa.eu/activities/risk-management/emerging-and-futurerisk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): „По отношение на архитектурата, при чувствителните приложения частните и обществени облаците се оказват решението, което в момента най-добре отговаря на нуждите на публичните администрации, тъй като те предлагат най-високо ниво на управление, контрол и прозрачност, въпреки че при планирането на частни или обществени изчислителни облаци трябва да се обърне специално внимание на мащаба на инфраструктурата."

[49] Нели Крус, заместник председател на Европейската комисия, отговаряща за цифровите технологии, Изграждане на Европейско облачно партньорство, Световен икономически форум в Давос, Швейцария, 26 януари 2012 г., URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ПРИЛОЖЕНИЕ

а) Базисни модели

Частният изчислителен облак[50] описва ИТ инфраструктура, която е предназначена за отделна организация; намира се в помещенията на организацията или нейното управление е възложено на трета страна (обикновено чрез хостинг сървър), която е под надзор на администратора. Частният облак може да бъде сравнен с конвенционалния център за данни - разликата е, че се прилагат технологични мерки за оптимизиране на използването на наличните ресурси и подобряването на тези ресурси чрез малки инвестиции, които са направени поетапно в хода на времето.

Публичният изчислителен облак, от своя страна, представлява инфраструктура, която е собственост на доставчик, специализиран в доставката на услуги, свързани с предоставянето - и следователно споделянето – на неговите системи с/между потребителите, стопанските предприятия и/или публичните административни органи. Услугите могат да са достъпни чрез Интернет, което води до прехвърляне на операции по обработка на данни и/или самите данни към системите на доставчика на услуги. Затова ролята на доставчика на услуги се приема като основна по отношение на ефективната защита на данните, налични в неговите системи. Заедно с данните, потребителят е длъжен да прехвърли голяма част от контрола си над тези данни.

Наред с „публичните" и „частните" облаци съществуват и така наречените „междинни" или „хибридни" облаци, където услугите, предоставяни от частни инфраструктури, съществуват съвместно с услугите, закупени от публични облаци. Трябва да се споменат и „общностните облаци", при които ИТ инфраструктурата се споделя от няколко организации в полза на конкретна потребителска общност.

Гъвкавостта и простотата при конфигурирането на облачните системи позволяват тяхното „еластично" оразмеряване, т.е. тези системи могат да бъдат адаптирани към конкретни изисквания на базата на ориентиран към използването подход. Не се изисква от потребителите да управляват информационните системи, използвани въз основа на споразуменията за аутсорсинг и напълно контролирани от тези трети страни, на чиито изчислителни облаци се съхраняват данните. Много често в процеса участват големи доставчици със сложни инфраструктури, което е причина облакът да обхване няколко местоположения и потребителите могат да игнорират точното местонахождение на съхранението на техните данни.

---

[50] Националният институт за стандарти и технологии (NIST) в САЩ, който от няколко години работи по стандартизацията на технологиите, базирани на изчислителните облаци[50] и чиито определения са посочени и в документа на Европейската мрежа и агенция за информационна сигурност (ENISA):
Частен изчислителен облак.
Инфраструктурата на облака се използва изключително за конкретната организация. Тя може да се управлява от организацията или от трета страна и може да съществува в помещенията или извън помещенията на организацията. Трябва да се отбележи, че „частният облак" разчита като минимум на определени технологии, които са типични и за „публичните облаци" – в това число, по-специално, виртуализационни технологии, които подпомагат реорганизацията (или основния ремонт) на архитектурата за обработка на данните, както е обяснено по-горе.
Публичен изчислителен облак.
Инфраструктурата на облака се предоставя на широката общественост или на голяма отраслова група и е собственост на организацията, продаваща услуги в облака.

б) Модели на доставка

В зависимост от изискванията на потребителите, на пазара се предлагат няколко решения за изчислителни облаци, които могат да бъдат групирани в три основни категории или „модели на услуги". Тези модели обикновено се прилагат, както за решенията за частни облаци, така и за публични облаци:

- **Инфраструктура на облака като услуга (IaaS - Cloud Infrastructure as a Service):** доставчикът предлага технологична инфраструктура, т.е. виртуални отдалечени сървъри, които крайният потребител може да използва в съответствие с конкретните механизми и договорености, при което те трябва да са прости, ефективни и способни да заменят корпоративните информационни системи в помещенията на компанията и/или да използват наетата инфраструктура заедно с корпоративните системи. Такива доставчици обикновено са участници на специализирания пазар и в действителност могат да разчитат на физически сложна инфраструктура, която често се простира в рамките на няколко географски области.
- **Софтуер на облака като услуга (SaaS - Cloud Software as a Service):** доставчикът осигурява чрез мрежата различни приложения и ги предоставя на крайните потребители. Тези услуги често са предназначени да заменят конвенционалните приложения, които са инсталирани от потребителите на техните локални системи и съответно потребителите в крайна сметка трябва да изнесат данните си на системите на конкретния доставчик. Такъв е случаят, например, с типичните уеб-базирани офис приложения, като например електронни таблици, инструменти за текстообработка, компютъризирани регистри и програми, споделени календари и т.н., при което въпросните услуги включват и приложения за електронна поща в изчислителния облак.
- **Платформа на облака като услуга (PaaS - Cloud Platform as a Service):** доставчикът предлага решения за усъвършенствано разработване и хостване на приложения. Тези услуги обикновено са адресирани към участници на пазара, които ги използват за разработване и хостване на патентовани базирани на приложенията решения, с цел да се осигури съответствие с вътрешните изисквания и/или за предоставяне на услуги на трети лица. И в този случай услугите, предоставяни от доставчиците на PaaS позволяват на потребителя да не използва допълнителен и/или специфичен хардуер или софтуер на вътрешно ниво.

Очевидно в краткосрочен план не е възможно пълномащабно преминаване към изцяло публична облачна система поради няколко причини, по-специално по отношение на големите предприятия, като например големи компании или организации, които изпълняват специфични задължения - например големи банки, правителствени органи, големи общини и др. Това може да се обясни с два основни фактора: първо, наличието на фактора инерция, който е свързан с инвестициите, необходими за постигане на такова преминаване; и второ, трябва да се вземе предвид особено ценната и/или чувствителната информация, която трябва да се обработва в конкретните специфични случаи.

Другият фактор, възпрепятстващ използването на частни облаци (поне в случаите, посочени по-горе), е свързан с обстоятелството, че никой доставчик на услуги в публичния облак не може да осигури постоянно качество на услугата (въз основа на споразуменията за нивото на обслужване - SLA), като например да е на ниво с критичния характер на услугите, които предлага администратора на данни - може би защото честотната лента и надеждността на мрежата не са достатъчни или не са подходящи в дадена област или по отношение на конкретните връзки потребител-

доставчик. От друга страна, може логично да се предположи, че в някои от горните случаи могат да се наемат частни облаци (защото това може да се окаже по-рентабилно), или пък да се използват модели на хибридни облаци (включващи публични и частни елементи). При всеки един от случаите трябва да се обсъдят внимателно съответните последици.

При липса на международно признати стандарти, съществува риск от използването на облачни решения от типа „направи си сам" или други комбинирани решения, което ще доведе до опасност от увеличаване на зависимостта на клиента (както и за явлението, наречено „конфиденциални монокултури")[51] и невъзможност за постигане на пълен контрол върху данните, без да се гарантира оперативната им съвместимост. Оперативна съвместимост и преносимост на данните наистина са ключови фактори за развитието на базираните на изчислителните облаци технологии, както и за осигуряване на пълното упражняване на правата за защита на данните, които субектите на данни имат (като например правото на достъп или коригиране).

От тази гледна точка, настоящият дебат относно технологиите на изчислителните облаци представлява съществен пример за напрежението, съществуващо между разходно-ориентираните и ориентираните към правата подходи, очертани накратко в раздел 2 по-горе. Докато използването на частни облаци може да е подходящо и наистина препоръчително от гледна точка на защитата на данните, като се вземат предвид конкретните обстоятелства на обработка на данните, този метод не е благоприятен за конкретната организация в дългосрочен план, най-вече в икономически ориентирана перспектива. Необходима е внимателна оценка на засегнатите интереси, тъй като в момента в тази област не може да се предложи универсално решение, което да е подходящо за всички случаи.

[51] Вж. проучването на Европейския парламент „Това помага ли или пречи? Насърчаване на иновациите в Интернет и правото на гражданите на неприкосновеност на личния им живот", публикувано през декември 2011 г.