ПРЕДИЗВИКАТЕЛСТВА, СВЪРЗАНИ СЪС ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ ПРИ ИЗПОЛЗВАНЕ НА „ОБЛАЧНИ“ (CLOUD) УСЛУГИ

адв. Десислава Кръстева

Фондация „Право и Интернет“

www.netlaw.bg

Така наречения ‘cloud computing’ („облачни“ услуги) съставлява набор от технологии и разнообразни модели на предоставяне на услуги с основен фокус върху Интернет-базираното използване и предоставяне на технологични приложения, възможности за обработване на информация и пространство за съхраняването й. „Облачните“ услуги често се представят като една от най-значимите технологични революции в последните години. Същите тези „облачни“ услуги, обаче, могат да се разглеждат не толкова като технологична революция, а като естествено продължение на развитието на добре познати класически технологични услуги.

Да се даде ясна и изчерпателна дефиниция на „облачните“ услуги е едва ли не невъзможно, а в голяма степен и ненужно. Най-специфичното за тях е именно техния комплексен, динамичен и разнообразен характер; гъвкавостта, с която се комбинира разнообразен набор от технологични решения и ресурси, за да се отговори на специфичните нужди на конкретен ползвател (клиент). Друга специфична характеристика на „облачните“ услуги е, че независимо от техните конкретни технологични компоненти, те поставят сходни правни предизвикателства в сферата на защитата на личните данни. Независимо дали говорим за „облачни“ услуги, предоставяни под формата на инфраструктура (IaaS, Cloud Infrastructure as a Service), на софтуер (SaaS, Cloud Software as a Service) или на платформа (PaaS, Cloud Platform as a Service), или за каквито да е други нови разновидности или комбинации от вече познати типове „облачни“ услуги, пред техните ползватели стои въпросът с осигуряване защитата на информацията им, в това число и на личните данни.

За целите на настоящото кратко изложение е важно да се подчертае, че предмет на разглеждане са само и единствено „облачни“ услуги/ технологии, предоставяни от външен доставчик. Доколкото при т. нар. „частни“ облаци, контролът и върху техническите ресурси (оборудването), и върху самата информация, която се обработва и съхранява на тях, е съсредоточен изцяло в конкретно дружество (администратор на данни), то липсват специфични правни предизвикателства, които да налагат по-различен подход от обичайните мерки за защита на данните.

По-отношение на всички „облачни“ услуги, при които е налице под каквато и да е форма участието на външен доставчик, обаче, възникват редица правни въпроси, които следва да бъдат решени, за да се спази приложимото в ЕС законодателство.

I. Предизвикателства при предоставянето на „облачни“ услуги

1. Външен доставчик

Едно от най-съществените предимства при ползване на „облачни“ услуги е възможността на относително ниска цена да се гарантира високо ниво на технологични мерки за защита на информацията. Днес пазарът на „облачни“ услуги е високо конкурентен и не липсват реномирани професионални доставчици на такива услуги, които разполагат с големи дейта центрове, в които се използват най-новите и усъвършенствани технологични мерки за защита на информация. От гледна точка физическа и технологична защита несъмнено тези доставчици предлагат възможно най-високото качество и дават възможност на своите клиенти да се възползват от едно изключително ниво на информационна сигурност, за многократно по-ниска цена от тази, която би била необходима, за да приложат същите технологии и защита локално на свои собствени сървъри, инфраструктури и платформи.

Същевременно използването на външен доставчик неминуемо намалява контрола на ползвателя върху обработваните от него данни и съответно върху тяхната защита. От правна гледна точка в резултат на достъпа и контрола, който има върху предлаганите от него услуги, инфраструктура, платформи и др. под., доставчикът на „облачни“ услуги се явява обработващ данните на ползвателя на услугата. Така, на практика, при всяко ползване на „облачни“ услуги компаниите предоставят данните на трети лица (доставчиците на „облачни“ услуги) и им възлагат да извършват определени действия по обработването им от тяхно име.

Много често тази специфика на „облачните“ услуги се пропуска или пренебрегва от администраторите на лични данни, тъй като официално достъп до данните имат само те с персонални пароли за достъп; осигурява им се проследимост на хронологията на достъпа и процесите с данните и не се извършва възлагане на конкретни задачи по обработване на тяхната информация в „облака“ към доставчика. Самият физически достъп до, поддръжката на и/или контролът върху оборудване, през което преминават лични данни или на което се съхраняват такива, обаче, може да се разглежда като обработване на личните данни, тъй като дори и самото съхраняване на данни е форма на обработване по смисъла на закона.

С други думи, ако „облачни“ услуги се ползват за целите на съхраняване или друга форма на обработване на лични данни, то:

1.1. Клиентът извършва трансфер на лични данни към лице, обработващо от негово име личните данни, а именно към доставчика на „облачната“ услуга;
1.2. Отношенията между клиента и доставчика, свързани с обработването на личните данни, следва да бъдат уредени в съответствие с изискванията на закона като отношения между администратор и обработващ, т.е. писмено да бъдат уредени задълженията на обработващото данните лице по защита на личните данни;
1.3. Клиентът като администратор на личните данни носи отговорността за защитата на тези данни с всички произтичащи от това задължения.

2. Международно-правен елемент

Към настоящия момент водещите доставчици на „облачни“ услуги са големи мултинационални компании. Този тип компании предлагат услугите си в цял свят; изграждат големи дейта центрове, в които се съхранява информацията на клиенти от различни държави; използват едно дружество за чисто търговските си отношения с клиентите, докато контрола върху самите дейта центрове е в друго дружество и т. н. Това внася международно-правен елемент в отношенията между клиентите и доставчиците на „облачни“ услуги и обуславя редица усложнения, свързани със защитата на данните, доколкото тяхното обработване се оказва предмет на уредба от различни юрисдикции.

Така на практика, ползването на „облачни“ услуги много често е свързано с необходимостта да се спази законодателството, свързано със защитата на личните данни при трансгранични трансфери. Допълнителен елемент на усложнение възниква в случаите, когато доставчикът е под юрисдикцията на трета страна, т.е. страна извън ЕС и/или ЕИП, а клиентът е лице от ЕС и/или ЕИП. В тези случаи клиентът е необходимо да предприеме допълнителни мерки, за да се гарантира, че доставчикът ще гарантира адекватно, съобразно европейските изисквания, ниво на защита на личните данни. За администратор, който извършва трансфери на лични данни към трети страни възникват и определени допълнителни административни задължения като уведомяване на съответния орган по защита на личните данни в неговата страна и др. под.

3. Подизпълнители

Друга типична специфика за дейността на доставчиците на „облачни“ услуги е използването на голям брой подизпълнители в различни юрисдикции. С цел оптимално използване на технологичните ресурси информацията динамично се прехвърля от едни сървъри на други, разположени в различни дейта центрове на различни локации и под контрола на различни лица (подизпълнители). В някои случаи подизпълнителите да лица от същата корпоративна група като основния доставчик, с който клиентът има договор, но в други се ползват и външни за

доставчика подизпълнители. Нещо в повече, с оглед минимизиране на разходите по предоставяне на такива услуги голям процент от подизпълнителите са установени на територията на трети за ЕС и ЕИП страни.

При класическия модел на предоставяне на „облачни“ услуги процесите по промяна на физическото местоположение на оборудването, използвано за съхраняване на информацията и смяната и/или ангажирането на подизпълнителите на доставчика се случва без знанието и извън контрола на клиента. Този класически модел на предоставяне на „облачни“ услуги, обаче, влиза в пряко противоречие с основните задължения на европейските администратори на лични данни, тъй като не позволява идентификация на обработващите данните лица, проследимост и контрол върху тяхната дейност, нито осигуряване на адекватно ниво на защита на личните данни в трети юрисдикции съобразно европейското законодателство.

4. Други предизвикателства

Към настоящия момент липсва специфична уредба, насочена конкретно към „облачните“ услуги. Те са предмет на общата уредба. Всъщност, подобно на опита да се даде изчерпателна дефиниция на „облачните“ услуги, една по-детайлна и специална уредба за същите вероятно би била или твърде непрецизна, или неактуална още от самото й създаване, заради многообразието от услуги, влизащи под общото название „облачни“ услуги и динамичните темпове на развитие.

Липсата на детайлна и специална уредба на „облачните“ услуги не е необходимо да се разглежда като пропуск на законодателя. Всъщност прекомерното регулиране на пазара и създаването на казуистична нормативна уредба би могло да има далеч по-негативно въздействие, от приложението на по-общи, технологично неутрални правила, дори и при създаването на последните „облачните“ услуги да не са съществували.

Същевременно, обаче, съществува определена нагласа, че липсата на специална уредба и необходимостта да се съблюдават общите принципи и правила, затруднява предлагането и ползването на „облачните“ услуги. Нерядко „остарялата“ уредба, непригодена към специфичните характеристики на „облачните“ услуги се посочва като основна пречка пред развитието им или като основно затруднение за участниците на този пазар (клиенти и доставчици). Особено осезаема е тази тенденция в сферата на защитата на личните данни.

Действително сега действащите правила по защита на личните данни в ЕС датират от 1995 г., момент, в който „облачните“ услуги не са съществували. В допълнение, тези правила на практика изключително формални и ограничителни в контекста на споменатия по-горе интернационален пазар, при който географското положение на данните не е от съществено значение. В тази връзка възниква въпросът, доколко една по-нова и специално насочена към „облачните“ услуги уредба би облекчила

предоставянето и ползването им и би преодоляла настоящите сочени за остарели и ограничителни правила.

II. Тенденции при трансферите на лични данни към трети страни

1. Трансграничен поток на данните

Технологично пред движението на данните днес няма ограничения. За крайния клиент технологично няма значение в коя точка на света се съхранява информацията, която той използва, нито къде се намира самия той, нито през колко юрисдикции същата преминава.

Например: Българско дружество – клиент на международен реномиран доставчик на „облачни“ услуги, сключва договор с ирландско дружество, което е част от корпоративната група на този доставчик. „Облачните“ услуги към българския клиент се предоставят основно чрез дейта центрове – един в Германия и друг в Румъния, които са съответно под контрола на немско и румънско дружество от корпоративната група на доставчика. За част от услугите, обаче, се ползват съоръжения в САЩ. В допълнение, част от поддръжката на съоръженията във всички тези страни и на предоставяните услуги, се извършва дистанционно от подизпълнители, които са извън корпоративната група на доставчика и извършват дейността си от Индия, Китай и Виетнам. Поддръжката на услугите им е възложена не пряко от ирландското дружество, което има договор с българския клиент, а от американското дружество. То има договор с китайска компания, която от своя страна превъзлага част от дейностите към подизпълнители в Индия и Виетнам. В допълнение, няколко месеца след сключване на договора доставчикът взима решение да премести предоставянето на услугите от немския и румънския дейта център, към дейта център в Унгария, и т. н., и т. н.

От технологична гледна точка клиентът би могъл да ползва услугите в пълен комфорт, без каквото и да е забавяне независимо, че са намесени множество юрисдикции. Нещо повече участниците в тази схема могат динамично да се променят без неговото знание и това по никакъв начин няма да се отрази на осезаемото за клиента качество на услугите. Всъщност това е един класически пример за механизъм, по който могат и се предоставят „облачни“ услуги.

От правна гледна точка, обаче, както вече посочихме преминаването на информацията (в това число лични данни) през множество юрисдикции е реално серия от трансфери на лични данни. И ако технологично това може да се осъществява все по-бързо и лесно, то по отношения изискванията за защита на личните данни тенденцията изглежда ориентирана в обратната посока. Законодател, институции и дори физическите лица, чиито данни се обработват, обръщат все по-голямо внимание и отдават все по-голямо значение на трансграничното движение.

2. Краят на Safe Harbor

Ключови в това отношение са две скорошни събития. Преди всичко, в края на 2015 година, в резултат на решение на Съда на Европейския съюз (СЕС) по дело C-362/14 един от инструментите за трансфер на лични данни към САЩ, а именно т.нар. решение за Safe Harbor, бе обявен за незаконен и съответно отменен. Това наложи всички субекти, които се ползваха с разрешенията и гаранциите на този инструмент за трансфери на данни от територията на Европейския съюз (ЕС) към САЩ, да преосмислят механизмите и основанията си за тези трансфери.

Прекият ефект от това решение е необходимостта от бързи промени в използваните инструменти за трансфер на лични данни от клиенти и доставчици на „облачни" услуги, т.е. бързо преуреждане на отношенията между тях, ако са разчитали на Safe Harbor. Далеч по-интересни са, обаче, самите мотиви на това решение, които сякаш повдигат фундаменталния въпрос относно ефективността на действащите инструменти за трансфери на лични данни. Ако същите се превърнат в трайна практика на СЕС и се започнат да се прилагат последователно и при други случаи на трансфери на лични данни към трети страни Safe Harbor няма да е единствения инструмент, който е негоден да осигури целеното от ЕС адекватно ниво на защита на личните данни трансферирани към трети страни. Това на практика би довело до радикални промени в механизма, по който се уреждат трансферите на лични данни.

Известно е и е отбелязано в решението, приложението на принципите на Safe Harbor в САЩ може да бъде ограничено, ако това е необходимо за целите на националната сигурност, обществения интерес или за да се спазят нормативни изисквания или ако е предвидено в закон, наредба, прецедент, които влизат в конфликт с тях. Съдът подчертава, че тези изисквания „имат приоритет над принципите на Safe Harbor и поради това самосертифицираните организации в САЩ … са задължени да не зачитат принципите (*на Safe Harbor)* без каквито и да е ограничения, ако те (*принципите)* са в конфликт с тези изисквания". Въз основа на тази констатация, наред с други аргументи и в контекста на наличната информация, че „американските власти могат да имат масов и несистематизиран достъп до личните данни на населението, живеещо на територията на Съюза", СЕС отменя решението за Safe Harbor.

Тази констатация, обаче, напълно валидна и за останалите налични инструменти за трансфер на лични данни към трети страни като стандартните договорни клаузи и дори за бъдещи такива като обвързващите корпоративни правила (Binding Corporate Rules). Без значение кой от тези инструменти се прилага, е обективно невъзможно чрез него да се преодолеят задължителните норми, установени в местното законодателство на третата държава, към която се извършва трансфер на лични данни. Получателят на данните в третата страна, независимо колко е добросъвестен и какви усилия полага за защитата на данните е безсилен пред разпорежданията на местните компетентни органи.

Така на практика става все по-очевидно, че опитът с договорни клаузи или други „soft-law" инструменти да се гарантира желаното от ЕС „адекватно ниво на защита на личните данни", трансферирани към държава, чието законодателство не гарантира такова „адекватно ниво на защита", е обречен на неуспех и е по-скоро в сферата на добрите пожелания.

Затрудненията, свързани с изпълнението на европейските изисквания за осигуряване на „адекватно ниво на защита на личните данни" във всяка една юрисдикция, към която те се трансферират, е добре познат на големите международни доставчици на „облачни" услуги. За да се намали административната тежест и да се избегнат или поне да се намалят трансферите на лични данни към трети страни, някои от тези доставчици са изградили дейта центрове на територията на ЕС, предназначени да обслужват преди всичко европейските клиенти. Едно друго относително скорошно събитие, обаче, заслужава по-специално внимание.

3. „Бягство" от националното законодателство на доставчика

През ноември 2015 г. бе оповестена новината, че американска мултинационална компания, която е и един от водещите доставчици на „облачни" услуги в света, изгражда нов дейта център в Германия, който ще бъде недостъпен за американските власти. Любопитното тук не е това, че се изгражда дейта център в Германия, вероятно почти всеки голям доставчик има такъв център в Германия, а механизмът, чрез който се този доставчик се стреми към пълното елиминиране на възможността американските власти да достъпват информацията, съхранявана в този дейта център. За целта самият дейта център ще бъде под контрола и ще се управлява от местно дружество, което е извън корпоративната група на доставчика. Така на практика доставчик на услугите за европейските дружества ще бъде не американската мултинационална компания, а немско дружество без каквото и да е международно участие, по отношение на което американските власти нямат възможност да прилагат американското законодателство. Макар да се използват технологиите, ноу-хау и стандарти за качество изградени от американската компания тя се отказва от контрола върху съоръженията и предоставянето на услугите, за да се гарантира, че американските власти няма да имат възможност да я принудят да им съдейства и да им предоставя достъп информацията на европейски клиенти.

Това събитие вероятно сочи още една тенденция, която е възможно да се развие в бъдеще. Не само трансфера (физически към сървъри) на данни извън държави от ЕС и ЕИП към трети страни би могъл да доведе до липса на „адекватно ниво на защита" на тези данни и да позволи на чуждестранни власти да осъществяват достъп до тях, а самият факт, че доставчик на „облачните" услуги е чуждестранно лице, което е субект на правото на трета страна или дори е местно лице, което обаче е част от корпоративната група на такова чуждестранно лице. За да се разбере по-

добре тази възможност е необходимо да се посочи, че в законодателството на определени държави съществуват разпоредби, които задължават местните дружества да им съдействат и да им предоставят информация, която е под контрола на техни дъщерни дружества установени в други държави. Така например едно американско дружество, което държи определен процент от капитала на едно немско дружество би могло да бъде задължено от американските власти да им окаже съдействие, за да могат те да достъпят информация, която е под контрола на немското дружество.

4. Остаряло ли е законодателството и това ли е проблемът, пред който са изправени „облачните“ услуги

Очертаните по-горе тенденции сочат, че към момента е трудно да се предвиди как ще се развият моделите на предоставяне на „облачни“ услуги в бъдеще. От една страна е факт, че сегашната уредба в ЕС налага сериозни изисквания и ограничения пред ползването на такива услуги с оглед задължението на клиентите като администратори на лични данни да осигурят и гарантират адекватното ниво на защитата на личните данни. От друга страна, обаче, облекчаване на тези изисквания би означавало отказ на ЕС от поставената от него цел да се гарантира адекватно ниво на защита на личните данни, което изглежда малко вероятно контекста на решението на СЕС за Safe Harbor. В допълнение самият пазар поставя своите изисквания – клиентите искат да се възползват от предимствата на „облачните“ услуги, а международните доставчици искат да предложат услугите си на платежоспособния европейски пазар и съответно търсят решения, които ще направят техните услуги достъпни и привлекателни за клиентите.

Макар примерите по-горе да са фокусирани основно върху конфликта в концепциите за защита на личните данни на САЩ и ЕС, то идентифицираните проблеми са общовалидни и важат за трансферите на данни към която и да е трета страна, която не осигурява „адекватно“ спрямо европейските изисквания ниво на защита на личните данни. Единствената причина първите проявления тези проблеми да са свързани с американски компании е изключително развитият IT сектор в САЩ и интензивните икономически отношения между САЩ и ЕС. Без значение къде е установен доставчикът на „облачни“ услуги, Китай, Индия, Русия, Япония, Турция, Виетнам, Южна Африка и т.н., и т.н., ако това е трета на ЕС страна и той и европейските му клиенти ще са изправени пред предизвикателството да осигурят адекватно ниво на защита на данните в юрисдикцията на трета страна.

Един по-задълбочен анализ на правната уредба и на идентифицираните затруднения пред предлагането и ползването на „облачни“ услуги позволява да се твърди, че всъщност основният проблем не се състои в „остаряла“ или „липсваща“ нормативна уредба, а в противоречия на концептуално ниво между правните системи на суверенни държави. В този смисъл едно обновяване на правната уредба фокусирано

върху технологичните особености на „облачните“ услуги реално не би могло да преодолее набелязаните проблеми.

III. Изисквания приложими към защитата на личните данни в „облака“

1. Нормативна уредба и помощни инструменти за уреждане на отношенията

Както бе посочено по-горе, макар да липсва подробна специална уредба относно „облачните“ услуги, то далеч не може да се твърди, че липсват правила за защитата на личните данни в „облака“. Към „облачните“ услуги с пълна сила се прилагат общите правила относно защитата на личните данни.

Дейността, свързана с предоставянето и ползването на „облачни“ услуги на национално ниво в България се регулира от множество разнообразни нормативни актове, включващи Закона за защита на личните данни, Закона за електронната търговия, Търговския закон, Закона за задълженията и договорите, както и от специалното секторно законодателство (Закон за електронните съобщения и др.). На европейско ниво понастоящем все още е приложима Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

Съществуват и редица международни документи, приложими в сферата като напр. Насоки за стандартни европейски SLA (т.е. споразумения за ниво на качество на услугата при предоставяне на „облачни“ услуги (Cloud Service Level Agreement Standardization Guidelines), както и различни стандарти и ръководства на организации като ENISA, NIST, ISO/IEC7. Тези документи могат да са в помощ както на доставчиците, така и на ползвателите на „облачни“ услуги при уреждане на отношенията им.

В допълнение, през ноември 2012 г. Работната група по чл. 29 от Директивата за защита на личните данни прие становище (Становище №05/2012) относно „cloud computing”. Работната група по чл. 29 е консултативен орган и няма законодателни правомощия. Издаваните от нея становища имат тълкувателен характер и отразяват възгледите на европейските органи по защитата на личните данни относно прилагането на нормативната уредба. В тази връзка, набелязаните в Становище №05/2012 изисквания следва да бъдат съобразени, доколкото не противоречат на императивни норми на местното законодателство на съответните администратори.

2. Мерки за защита на личните данни в „облака“

В Становище №05/2012 се подробно разяснява какви конкретни действия и мерки е необходимо да предприеме един администратор, използващ „облачни“ услуги, за да се счете, че съблюдава изискванията на уредбата относно личните данни. Същите

са базирани основно на конструкция, при която отношенията „клиент-доставчик“ са отношения между „администратор и обработващ“. Подчертава се, обаче, че е възможно в определени случаи доставчикът на „облачни“ услуги да действа и като администратор, ако обработва допълнително лични данни предоставяни му от клиента за свои собствени цели.

Сред най-съществените изисквания, набелязани от Работната група по чл. 29 могат да се посочат следните:

- Клиент-администратор: Клиентът на „облачни“ услуги носи отговорност за защитата на личните данни, които се обработват чрез тези услуги като администратор на лични данни. Поради това клиентът е необходимо да избере доставчик, който гарантира спазването на европейското законодателство за защита на личните данни и това да бъде отразено в адекватни договорни гаранции и задължения.

- Подизпълнители: В случай, че доставчикът ползва подизпълнители е необходимо да се гарантира, че на тях ще им бъдат вменени задължения по защита на личните данни, които кореспондират със задълженията вменени от клиента към доставчика. Такива подизпълнители могат да се ползват само със знанието и съгласието на клиента, който трябва да разполага с информация идентифицираща всеки един от тези подизпълнители. В допълнение, клиентът е необходимо да може по всяко време да изиска преустановяване ползването на определен подизпълнител по отношение на предоставяните му услуги.

- Прозрачност: Клиентът трябва да разполага с пълна информация относно релевантните за защитата на данните аспекти и по-конкретно за всички подизпълнители, за всички места (локации), на които може да се съхранява негова информация (особено ако са извън ЕС/ЕИП), за прилаганите от доставчика технически и организационни мерки за защита на данните. В допълнение клиентът следва да информира физическите лица, чиито данни обработва, за факта на предоставяне на данните им към обработващи данните трети лица и за тяхното местоположение.

- Целево обработване на данните: Клиентът трябва предприеме мерки, с които да се гарантира, че личните данни няма да бъдат обработвани от доставчика и/или неговите подизпълнители за допълнителни цели, извън възложените им от него самия.

- Заличаване на данните: Необходимо е да се гарантира, че личните данни се заличават незабавно след постигане на целите за обработването им.

- Договорни механизми за защита: Договорът между доставчика и клиента е необходимо да е писмен и да предвижда ефективни мерки и механизми за защита на данните с адекватна отговорност на доставчика в случай на неизпълнение.

- Технически и организационни мерки за защита: Договорът е необходимо да съдържа детайлно описание на техническите и организационните мерки за защита на данните, които доставчикът ще прилага.

- Достъпност на данните: Достъпът до данните трябва да е ограничен единствено до надлежно оторизирани лица. Същевременно клиентът следва да си гарантира навременен и надежден достъп до данните.

- Интегритет на данните: Необходимо е да се гарантира интегритетът на данните и по-конкретно, при ползване на услугите същите трябва да са защитени срещу неоторизирано или случайно изменение или заличаване.

- Поверителност: Доставчикът, неговите служители, неговите подизпълнители, както и техните служители е необходимо да бъдат обвързани със задължение да пазят поверителността на данните и да не ги разкриват на трети лица.

- Подсигуряване на възможността лицата, чиито лични данни се обработват да упражняват всички свои права по отношение на тези данни: Доставчикът е необходимо да бъде обвързан от задължения за съдействие на клиента с оглед упражняването на правата на физическите лица, чиито данни се обработват (напр. правото им на достъп и корекция на данните).

- Преносимост/ Оперативна съвместимост: Клиентът е необходимо да си гарантира, че има контрол върху своята собствена информация и включените в нея лични данни. Този контрол включва и възможността при прекратяване на отношенията си с доставчика клиентът да има възможност да прехвърли информацията към друг доставчик или на свои собствени съоръжения. Тази възможност практически би могла да бъде ограничена или дори напълно блокирана, ако доставчикът не ползва стандартни формати за обработване и съхраняване на информацията или интерфейсите му не са оперативно съвместими с интерфейсите, използвани от клиента или от новите му доставчици на „облачни“ услуги.

- Контрол и отчетност/ Одити: В отношенията между клиент и доставчик е необходимо да се предвидят ефективни механизми за контрол от страна на клиента към доставчика за спазването на изискванията за защита на личните данни.

- Осигуряване на адекватно ниво на защита на личните данни при трансфери към трети страни: В случай, че ползването на услугите е свързано с трансфер

на данните към трети страни, то е необходимо в договорните отношения между клиент и доставчик да са уредени и конкретни мерки за осигуряване на „адекватно“ съобразно европейското законодателство ниво на защита. Това може да стане чрез включване на стандартните европейски договорни клаузи или по друг начин.

- Други.

В заключение въз основа на набелязаните по-горе конкретни изисквания може да се твърди, че към този момент за европейските администратори използването на „облачни“ услуги, предоставяни от международен доставчик, който не е установен на територията на ЕС/ЕИП или дори и да е установен на територията ЕС/ЕИП използва подизпълнители в трети страни или услугите му по друг начин предполагат трансфериране на информацията на клиентите към трети страни, е свързано със значителни затруднения. Такива клиенти е необходимо да положат значителни усилия, за да проверяват и контролират дейността на доставчика си и за да уредят детайлно отношенията си него по изисквания от европейското законодателство начин. Дори и след тези усилия, обаче, съществува риск с личните данни да бъде злоупотребено, до тях да бъде осъществен неправомерен от гледна точка на европейското право достъп и правата на физическите лица да бъдат накърнени. Този риск стои дори и при избор на реномиран и добросъвестен доставчик. Това от своя страна означава и риск от ангажиране отговорността на клиентите-администратори на лични данни и генерално поставя под въпрос възможността им да ползват подобни услуги.