EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers
Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Насоки на CCBE относно използването на изчисления в облак от адвокатски колегии и адвокати

27/02/2025

Съдържание

I. Въведение

1. Обхват на насоките

Тези насоки имат за цел да се повиши осведомеността относно различните рискове, свързани с използването на изчисления в облак в правната практика. Налице беше необходимост от актуализация на предходната версия от 2012 г., за да се отразят промените в законодателството, технологичното развитие и юридическата практика. Насоките също така имат за цел да дадат повече контекст на адвокатските колегии с оглед на използването от тях на облачни услуги. Те са предвидени за адвокатските колегии и правните общества, които членуват в CCBE, и са предназначени да ги подпомогнат при оказване на подкрепа на членовете им.

2. Контекст

През последните години използването на изчисления в облак и облачни услуги се увеличава.[1] През 2023 г. 42,5% от предприятията в ЕС са закупили услуги за изчисления в облак, най-вече за електронна поща, съхранение на файлове и офис софтуер. През 2023 г. делът на предприятията, които купуват изчислителни услуги в облак в ЕС, се е увеличил с 4,2 процентни пункта спрямо 2021 г.[2]

През 2022 г. CCBE проведе проучване за използването на изчисления в облак от адвокати.[3] Макар повечето адвокатски колегии да не разполагат с количествена информация за използването на изчисления в облак от адвокатските кантори, много от тях отчитат, че това използване се увеличава.

В САЩ данните в доклада за изчисленията в облак на Американската асоциация на юристите за 2023 г. *„отразяват значително увеличение на използването на изчисления в облак от адвокатите при практикуване на право. По данни от доклада за 2022 г. използването на облачни услуги се е увеличило значително от 60% на 70%. Водеща роля имат самостоятелните адвокати (увеличение от 52% до 84 % за една година), следвани от малките и средните адвокатски кантори (приблизително 75% спрямо около 65%)“.*[4]

[1] The State of Cloud Computing in Europe and the UK, Kinsta, accessed in January 2024
[2] Eurostat, Enterprises buying cloud computing services, EU, 2021 and 2023
[3] В проучването на CCBE отговори изпратиха 17 делегации: Австрия (AT), Хърватия (CO), Чехия (CZ), Дания (DE), Естония (ES), Франция (FR), Германия (GE) (отговор от Deutscher Anwaltverein), Гърция (GR), Унгария (HU), Ирландия (IR), Италия (IT), Лихтенщайн (LIE), Литва (LIT), Португалия (PO), Испания (SP), Швеция (SW) и Обединеното кралство.
[4] American Bar Association (ABA), 2023 Cloud Computing TechReport, January 2024

Изчисленията в облак предлагат многобройни предимства като например по-устойчиви устройства и резервни копия и възможност за достъп до данни от различни места и различни устройства (смартфони, лаптопи, компютри, таблети и др.), което е особено полезно при работа от разстояние и в сътрудничество. Така се осигурява и достъп до услуги, които могат да бъдат достъпни само в облачна среда[5], заедно с увеличено пространство за съхранение и изчислителна мощност. В допълнение, работата в облак може да предложи усъвършенствани решения за сигурност и по-голяма гъвкавост за потребителите. От друга страна, събирането, съхраняването и обработването на данни в облачна среда, особено когато тя се намира в чужбина, носи определени рискове.

3. Какво представляват изчисленията в облак?

Изчисленията в облак представляват общ термин за ИТ инфраструктура, която включва съхраняване и обработка на данни и софтуер от разстояние в център за данни на доставчика на облачни услуги или във взаимно свързани центрове, достъпни като услуга чрез интернет. Също така следва да се има предвид, че в днешно време изчисленията в облак не се отнасят само до съхранението на данни, но и до предоставянето на ИТ услуги, които се изпълняват в облака, а не на локален сървър, поддържан от потребителя, включително адвокати и служители на адвокатски дружества (например услуги за изпращане на съобщения до клиенти, инструменти за видеоконферентна връзка и др.).

Според Националния институт на САЩ по стандартизация и технологии (NIST) изчисленията в облак позволяват *„обхватен, удобен мрежов достъп по заявка до споделен пул от подлежащи на конфигуриране изчислителни ресурси (напр. мрежи, сървъри, хранилища, приложения и услуги), които могат да бъдат бързо предоставени и разпространени с минимални усилия за управление или взаимодействие с доставчика на услуги“*[6]. До голяма степен това определение се приема на международно ниво, включително от Международната организация по стандартизация (ISO)[7] и Европейския банков орган[8].

В ЕС обаче някои от най-новите правни актове на Съюза не се основават на това определение. Например в член 2, параграф 6 от Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 година относно авторското право и сродните му права в цифровия единен пазар и за изменение на директиви 96/9/ЕО и 2001/29/ЕО е дадено определение за „доставчик на онлайн услуга за споделяне на съдържание“, което се основава на определението за по-широкото понятие „услуга на информационното общество“ и се отнася до облачните услуги (без да им се дава

[5] Например инструменти за превод на различни езици.
[6] NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011
[7] ISO/IEC 22123-1:2023(en) Information technology — Cloud computing — Part 1: Vocabulary
[8] EBA Recommendations on Cloud Outsourcing and the forthcoming Guidelines on Outsourcing Arrangements (2018)

определение) като пример за такава услуга. По подобен начин правните определения в актове като Регламента за цифровите услуги (или Регламента относно платформа-към-бизнес (Регламент (ЕС) 2019/1150) също се основават на услугата на информационното общество, а не на по-малко правния, но по-технически или ежедневен термин „изчисления в облак“.

Като се имат предвид тези моменти, настоящите насоки не въвеждат ново или ревизирано определение за изчисления в облак. Вместо да се поставя акцент върху конкретния термин, по-важно е да се обърне внимание на различните рискове, които използването на облачни услуги може да носи за адвокатите и техните клиенти.

4. Какви са разпоредбите в ЕС относно изчисленията в облак?

Съществуват редица закони и разпоредби, които засягат начина, по който бизнес процесите могат да се възлагат на доставчици на услуги за изчисления в облак. От гледна точка на професионалните задължения на адвокатите ключовата характеристика на облачните услуги е обработката на данни от трети страни, която вероятно включва кореспонденция между адвокатите и техните клиенти и друга обработка на лични данни.

На равнище ЕС защитата на поверителността на комуникацията между адвокат и клиент е призната като общ принцип на правото на ЕС от Съда на Европейския съюз и има правно основание в Хартата на основните права на ЕС в чл. 7 относно правото на зачитане на личния живот и чл. 47 относно правото на справедлив съдебен процес. Ако правото на поверителна комуникация с адвокатите не е гарантирано, клиентите може да нямат доверие да разкрият напълно информацията, необходима на адвоката да предостави точен правен съвет и представителство в отговор на ситуацията на клиента. С други думи, правото на клиентите на правен съвет и на справедлив съдебен процес ще бъде сериозно накърнено.

В Европа чл. 8 от Хартата на основните права на Европейския съюз предвижда защита на личните данни, а чл. 6 – правото на справедлив съдебен процес.

Основният законодателен акт на ЕС, уреждащ обработването на лични данни, е Общият регламент относно защитата на данните (ОРЗД | GDPR)[9], актовете за неговото прилагане в държавите членки и свързаните с тях насоки на Европейския комитет по защита на данните (ЕКЗД). Те обаче не се отнасят конкретно до адвокатите и техните задължения, а имат по-скоро по-общо приложение.

[9] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните): https://eur-lex.europa.eu/eli/reg/2016/679/oj

ОРЗД предвижда правните основания за обработване на лични данни, правата на субектите на данни, задълженията на администраторите и обработващите лични данни, изискванията за информационна сигурност, оценките на риска и въздействието и международното предаване на данни. По-голямата част от задълженията са на така наречените „администратори на данни“. Адвокатите следва да приемат, че са администратор на данни в условията, когато предоставят правни услуги или изпълняват собствените си регулаторни задължения.[10]

Важно е да се отбележи, че изискванията за международното предаване на данни, посочени в глава V от ОРЗД, са от особено значение за облачните услуги, тъй като те могат да бъдат физически базирани извън ЕС/ЕИП и по този начин да породят множество задължения за организациите, които използват такива услуги, включително адвокати и адвокатски кантори. Това е така, тъй като доставчиците на услуги, базирани в юрисдикции извън ЕС/ЕИП, подлежат на различни разпоредби и като такива те могат да позволят поведение, което би застрашило спазването на националните или европейските разпоредби от страна на адвокатите и адвокатските кантори. Важен пример са разпоредбите, които задължават правоприлагащите и разузнавателните органи на трети държави да имат достъп до данни, съхранявани от дружества, попадащи под тяхната юрисдикция, което може да повлияе на поверителността на данните, съхранявани от въпросния доставчик.

5. Чуждестранни закони, приложими към данни

Когато данни се съхраняват или обработват в юрисдикция, различна от тази на адвоката, възниква въпросът кои закони се прилагат за тях. Това е още по-важно, когато данните се съхраняват извън ЕС/ЕИП и дали съгласно правото на ЕС на данните се осигурява равностойна защита на тази, която се прилага в ЕС/ЕИП. Адвокатите, които обмислят доставчици на услуги за изчисления в облак в САЩ, трябва да обърнат внимание на решенията на Съда на ЕС (СЕС) по делата Schrems I и Schrems II, свързани с механизмите за предаване на данни между ЕС и САЩ. По делото Schrems II Съдът обявява решението на Европейската комисия за Щит за защита на личните данни за невалидно поради инвазивните програми за наблюдение на САЩ, като по този начин предаването на лични данни въз основа на решението за Щит за защита на личните данни става незаконно. В допълнение това Съдът определя по-строги изисквания за предаването на лични данни въз основа на стандартни договорни клаузи (СДК).[11] Европейската комисия издаде решение за адекватност на предаването на лични данни между ЕС и САЩ, при условие че получателят на данни от САЩ се придържа към Рамката за защита на личните данни – продължение на вече несъществуващия Щит за защита на личните данни. Съответно на адвокатите, които разчитат на доставчици на

[10] Европейски комитет по защита на данните, 7 юли 2021 г., Guidelines 07/2020 on the concepts of controller processor in the GDPR

[11] За повече подробности относно решението по делото Schrems II вижте: The CJEU judgment in the Schrems II case, European Parliament Research Service, 2020

услуги в САЩ, се препоръчва да въведат резервен механизъм за прехвърляне на данни чрез т.нар. стандартни договорни клаузи (СДК) – набор от примерни договорни клаузи, които са били „предварително одобрени“ за адекватност от Европейската комисия.

6. По-широк контекст от гледна точка на правото и политиките

Различни аспекти на облачните услуги се регулират от няколко законодателни акта:

- Директива за мрежовите и информационните системи (МИС2) (2022)[12] (законодателство в ЕС относно киберсигурността);
- Регламент относно свободното движение на нелични данни (2018)[13] (има за цел да премахне пречките пред свободното движение на нелични данни между различни държави от ЕС и ИТ системи в Европа);
- Акт за киберсигурността (2019)[14] (укрепва Агенцията на ЕС за киберсигурност (ENISA) и създава рамка за сертифициране на продукти и услуги в областта на киберсигурността);
- Акт за данните (2023)[15] (инициатива за справяне с предизвикателствата и разгръщане на възможностите, които предоставят данните в Европейския съюз);
- Акт за изкуствения интелект (Акт за ИИ) (широка законодателна рамка, която да регулира предоставянето и внедряването на системи с ИИ);
- Акт за киберустойчивост (друга законодателна рамка, насочена към повишаване на киберсигурността на хардуерни и софтуерни продукти с цифрови компоненти).

ЕС също така създава или подпомага редица работни групи, в резултат на чиято работа са определени различни доброволни кодекси за поведение и механизми за сертифициране. Сред тях са Насоките за стандартизиране на споразуменията за ниво на обслужване в облака (2014) на Специализираната група за облачни услуги (C-SIG)[16] или работната група „Смяна на доставчика на облачни услуги и пренасяне на данни“ 7,

[12] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2), ОВ L 333 27.12.2022, стр. 80: https://eur-lex.europa.eu/eli/dir/2022/2555

[13] Регламент (ЕС) 2018/1807 на Европейския парламент и на Съвета от 14 ноември 2018 година относно рамка за свободното движение на нелични данни в Европейския съюз, ОВ L 303, 28.11.2018, стр. 59–68: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

[14] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността), ОВ L 151, 7.6.2019, стр. 15–69: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[15] Регламент (ЕС) 2023/2854 на Европейския парламент и на Съвета от 13 декември 2023 година относно хармонизирани правила за справедлив достъп до данни и за тяхното използване и за изменение на Регламент (ЕС) 2017/2394 и Директива (ЕС) 2020/1828 (Акт за данните), ОВ L 2023/2854, 22.12.2023: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854&qid=1717084009218

[16] Насоки за стандартизиране на споразуменията за ниво на обслужване в облака: https://digital-strategy.ec.europa.eu/en/news/cloud-service-level-agreement-standardisation-guidelines

която определя подробни изисквания за експортиране и импортиране на данни от облака, когато потребителят желае да премине към друг доставчик. Ето примери за кодекси за поведение:

- Кодекс за поведение на SWIPO SaaS за преносимост на данните за собствените данни на адвокати[17]
- Кодекс за поведение в облака на ЕС, схеми за киберсигурност и сертифициране (свързани с проблеми при преговори, които не са специфични за адвокати, а са общи за всички МСП).[18]

7. Какви са рисковете при използването на изчисления в облак от адвокати?

Основният риск, свързан с използването на услуги в облак, произтича от факта, че данните се обработват от трета страна доставчик, който може да е възложил част от обработката на други трети страни, като всички те могат да се намират в чужбина, включително извън ЕС/ЕИП. Оттук възникват въпроси относно:

- контрола от страна на адвоката или адвокатското дружество върху техните данни и данните на техните клиенти като например наличност и достъп до данните и предоставените услуги, поддържане на подходящи записи за дейностите в съответствие с регулаторните задължения или осигуряване на непрекъснатост на професионалната практика и ефективно възразяване срещу обработването;
- поверителния и привилегирован характер на обработваните данни и потенциалната заплаха за тях чрез загуба, кражба и законно или незаконно разкриване; особено поради факта, че дейностите на редица адвокати представляват интерес за злонамерени лица; и
- как да се гарантира точността, пълнотата и качеството на данните, възложени на множество доставчици на услуги за изчисления в облак и съхранявани във времето и в различни формати (цялостност).

Сред трите най-големи опасения, свързани с използването на облачни услуги, посочени от членовете на CCBE в проучването от 2022 г., са защитата на поверителността, контролът на данните и цялостната киберсигурност.

Тези рискове могат да възникнат в множество ситуации и в резултат на:

[17] https://swipo.eu/saas-sector-group/
[18] https://eucoc.cloud/en/home

- непознаване на възможностите на облака и техническите тънкости (напр. отдалечено съхранение на данни, договорни ограничения на някои функционалности като резервно копие и достъп до данни, криптиране и др.);
- неразбиране на моделите за доставка на облачни услуги, включително дистрибуторите с добавена стойност и допълнителните нива на сложност на договорите, напр. дълга верига на доставки и множество партньори, използвани от доставчиците на облачни услуги;
- недостатъчно познаване на доставчика на услуги, а именно финансов риск от загуба на предварително платените абонаментни такси и потенциална загуба на данни, обработвани от доставчика;
- недостатъчна защита на киберсигурността от страна на потребителя (т.е. на адвокатите) (напр. недостатъчно внимание при поддържането на данните за вход в иначе сигурна услуга за изчисления в облак или използване на т.нар. сенчести ИТ);
- недостатъчно познаване на законите и разпоредбите, които се прилагат за обработката на данни и за достъпа до данни от правоприлагащите органи, особено в чуждестранни юрисдикции, или за по-нататъшната обработка на данни от доставчиците на облачни услуги; или
- технически проблеми и липса на одобрение от страна на потребителите във връзка с функционалност, използваемост или проблеми с достъпността (напр. услугата не разполага с всички необходими функции или не може да се използва от адвокати с увредено зрение);
- липса на разбиране на правилата и условията за ползване поради ниската прозрачност на доставчиците (в съчетание с относителната лекота на използване и достъпност на решенията);
- липса на задълбочен преглед на условията за ползване и съответната договорна документация.

II. Насоки на CCBE относно използването на изчисления в облак от адвокати

Когато предоставят съвети на своите членове, които обмислят внедряване на изчисления в облак в своята практика, националните адвокатски колегии и правни общества следва да привлекат вниманието им и към съображенията по-долу.

1. Професионални задължения

Използването на услуги за изчисления в облак засяга прилагането на няколко основни принципа на юридическата професия, както е посочено в Хартата на основните

принципи на европейската правна професия на ССВЕ и в Примерния кодекс за поведение на ССВЕ, а именно поверителност и професионална компетентност.

Поверителност

Адвокатите са длъжни да пазят в тайна комуникацията си с клиентите, информацията, получена от тях, и съветите, дадени на клиентите им. Поверителността на комуникациите между клиента и неговия адвокат е защитена по силата на принципа на професионалната тайна (известен също като „правна професионална привилегия“), който се прилага и за онлайн комуникациите.[19]

Основният принцип (b) на Хартата на европейската правна професия на ССВЕ се отнася до *„правото и задължението на адвоката да пази поверителността на делата на клиентите и да спазва професионалната тайна (и произтичащата от това необходимост да полага разумни усилия за предотвратяване на неразрешен или незаконен достъп до поверителна информация)“*.

В член 1 от Примерния кодекса за поведение на ССВЕ, посветен на поверителността, е предвидено: *„Адвокатът е обвързан с поверителност. Тя е задължение на адвоката, а може да бъде и негово право“*. Точка 4 от същия член гласи: „*Поверителността се отнася за всяка и всякаква информация относно клиент или въпрос на клиент, която е предоставена на адвоката от неговия клиент или която е получена от адвоката в хода на упражняването на професията му, независимо от източника на тази информация“*. Точка 5 предвижда: *„Поверителността се отнася за всеки и всички документи, изготвени от адвоката, за всички документи, предоставени от адвоката на неговия клиент, и за всички съобщения между тях.“ „Адвокатът е длъжен да спазва поверителността на всяка информация, която му е станала известна в хода на професионалната му дейност.“*

Професионална компетентност

Адвокатите са длъжни да актуализират и поддържат своите знания и професионални умения. Основният принцип (g) се отнася до *„професионалната компетентност на адвоката (и произтичащата от това необходимост от осведомяване за най-новите технологични постижения и тяхното въздействие върху адвокатската практика и професионалните задължения на адвоката)“*.

В т. 2.2 от примерния член за отношенията с клиентите е предвидено: *„Адвокатите поддържат професионалните си умения чрез продължаващо обучение по правни и други свързани с практиката въпроси“*. В същата точка се пояснява, че: *„Компетентното представителство изисква правни познания, умения, задълбоченост*

[19] Повече информация за поверителността на комуникацията между адвокати и клиентите вижте в: ‘Confidentiality of lawyer-client communications: a must for protecting your rights (2023)’

и подготовка, които са разумно необходими за представителството. Адвокатите са в състояние да осигурят такова компетентно представителство само като са в крак с непрекъснатите бързи промени в правото и технологичната среда, в която работят“.

Така, задължението за компетентност на адвоката не се ограничава само до правото и нормативната уредба, а включва и задължението за познаване на технически продукт, който ще се използва за професионалната дейност. В настоящия контекст тези знания могат ефективно да помогнат на адвоката да оцени и намали рисковете, свързани с използването на облачни услуги.

2. Разбиране на рисковете, свързани с използването на изчисления в облак

Важно е адвокатите да анализират и оценяват рисковете на конкретните продукти и услуги, които възнамеряват да използват. Въз основа на резултатите от тази оценка адвокатите трябва да прилагат необходимите мерки за намаляване на рисковете и да потърсят допълнителен съвет, когато е необходимо. Целта да се оценят и управляват рисковете при използването на услуги за изчисления в облак важи за адвокатски кантори от всякакъв мащаб – малки и големи. От друга страна, източниците на рискове, които трябва да бъдат оценени, подробностите по оценката и възможните мерки за намаляване на рисковете зависят както от вида и размера на адвокатската кантора, така и от областта, в която тя работи.

Адвокатите трябва непрестанно да се информират, например чрез съответни обучения, за да поддържат актуални знанията си за приложимите закони и разпоредби относно изчисленията в облак, киберсигурността, както и за професионалните задължения в тези области. Адвокатските колегии и правните общества следва да предоставят на адвокатите възможности да получават съответната информация и обучение в тези области.

3. Осигуряване на съответствие с етичните правила и законите за защита на данните

Адвокатите трябва да полагат разумни усилия да преглеждат и разбират както съответните закони, така и националните професионални задължения във връзка с използването на данни на клиенти, преди всичко за да предотвратят неразрешен или незаконен достъп до поверителна информация и информация, която е предмет на професионална тайна/правна професионална привилегия. По-специално, адвокатите следва да проверят дали съгласно приложимите етични правила им е разрешено да съхраняват данни извън своята адвокатска кантора и ако това е така, да се уверят, че доставчикът на услуги за изчисления в облак не е в юрисдикция, която позволява упражняване на права спрямо неместно лице, при което ще е налице задължение да

предаде данните на европейски адвокати, съхранявани на сървър в облак, на национални органи извън ЕС в зависимост от случая.

Това включва цялостно разбиране и спазване на Общия регламент относно защитата на данните (ОРЗД), като се обръща особено внимание на правилата, приложими към администраторите, обработващите лични данни, сигурността на данните и правата на субектите на данни, както и на правилата за трансгранично предаване и съхранение на данни.

Това включва задължението за уведомяване на клиента за всяко нарушение на сигурността на данните, когато това е уместно и след консултация с неговото длъжностно лице по защита на данните или националния орган за защита на данните, както и за предприетите стъпки за намаляване на вредите и предотвратяване на бъдещи инциденти.

4. Спазване на публикуваните насоки

Адвокатите трябва да следват насоките, предоставени от регулаторните органи, адвокатските колегии и правните общества. През последното десетилетие ССВЕ също публикува редица насоки, които могат да бъдат полезни за адвокатите, които използват услуги за изчисления в облак. Те включват:

- Препоръки относно защитата на поверителността на клиентите в контекста на дейностите по наблюдение (2016)
- Насоки на ССВЕ за подобряване на ИТ сигурността на адвокатите срещу незаконно наблюдение (2016)
- Насоки на ССВЕ за адвокати, които използват онлайн правни платформи (2018)
- Насоки за използване на инструменти, базирани на изкуствен интелект, от адвокати и правни фирми в ЕС (2022)
- Насоки на ССВЕ относно използването на инструменти за дистанционна работа от адвокати и дистанционно провеждане на съдебни производства (2020)
- Анекс към Насоките на ССВЕ относно използването на инструменти за дистанционна работа от адвокати и дистанционно провеждане на съдебни производства: Анализи на видеоконферентни инструменти (2020)

ССВЕ публикува два пакета насоки във връзка с ОРЗД:

- Препоръки във връзка с прилагането на Общия регламент относно защитата на данните (ОРЗД), които подпомагат адвокатските колегии и правните общества при подготовката за въздействието на националните различия, засягащи начина, по който адвокатите следва да работят по време на усилията за прилагане на регламента.

- Насоки за основните нови мерки за съответствие за адвокати във връзка с Общия регламент относно защитата на данните (ОРЗД), които предоставят преглед на основните нови мерки за съответствие, които адвокатските колегии и правните общества могат да препоръчат, за да гарантират спазването на изискванията, предвидени в ОРЗД.

5. Осигуряване на подходяща информационна сигурност

Независимо от естеството на работата си или размера на практиката си, адвокатите трябва да разполагат с мерки за сигурност, за да защитят своите ИТ системи, включително сигурността на комуникацията с клиенти и съхранението на данните на клиенти.

От адвокатите, които работят с голям брой частни клиенти и клиенти от малкия бизнес, се очаква да използват инструменти, които са съвместими с решенията, използвани от техните клиенти. Такива фирми трябва да обърнат внимание на скритите разходи за оперативна съвместимост и киберсигурност, като например загубата на гъвкавост по отношение на това какви ИТ продукти могат да използват поради съображения за сигурност, трудностите при използването на ИТ активите, които клиентите предоставят, разходите за допълнително конфигуриране и текущо обучение на служителите, редовните актуализации на функциите в облачните услуги, нарушаващи съвместимостта, и т.н.

Адвокатите следва да обмислят възможността да изискват от своите доставчици да спазват приложимите стандарти за ИТ сигурност, например тези, разработени от Международната организация по стандартизация (ISO), или стандартите за контрол на системите и организациите (SOC), разработени от Американския институт на дипломираните експерт-счетоводители:

- SO/IEC 27001:2022 – Сигурност на информацията, киберсигурност и защита на личните данни – Системи за управление на сигурността на информацията – Изисквания
- ISO/IEC 27017:2015 – Информационни технологии – Методи за сигурност – Кодекс за добра практика за управление на сигурността на информацията, базиран на ISO/IEC 27002 за услуги в облак
- ISO/IEC 27018:2019 – Информационни технологии – Методи за сигурност – Кодекс за добра практика за защита на личната информация за идентифициране (ЛИИ) в обществени облаци, действащи като обработващи лични данни[20]

[20] Към момента на изготвяне на документа между юни и октомври 2024 г. стандартът е в процес на преразглеждане.

- ISO/IEC 27036-4:2016 – Информационни технологии – Методи за сигурност – Сигурност на информацията при взаимоотношенията с доставчиците, Част 4: Насоки за сигурност за услуги в облак
- SOC 2 – SOC for Service Organisations: Критерии за доверителни услуги и сигурността на информацията не се ограничават само до технически мерки и следва да включват съответните политики и организационни практики, за да се гарантира сигурността на информацията и данните, обработвани от практиката.

В допълнение, адвокатите следва да имат предвид, че статусът на сертификация (за ISO) се преразглежда периодично и че се изискват нови атестации (за SOC2), както и да разбират кои документи са полезни за оценката на риска.

6. Познаване на доставчика на облачни услуги и на неговите продукти/услуги

Преди да използват услуги за съхранение и други услуги в облак, адвокатите трябва да извършат оценка на риска и внимателно да изберат доставчика на услуги. По-специално, адвокатите следва да извършат квалифицирана комплексна проверка на правните гаранции, предлагани от доставчика, когото възнамеряват да ангажират за предоставяне на облачни услуги, попадащи в обхвата на професионалната тайна/поверителност. В тази дейност предвид следва да бъдат взети няколко основни вида информация, изброени по-долу. Тази информация може да бъде включена в договора, общите условия за ползване на услугата, съобщенията за поверителност, съобщенията за „бисквитки“ или в технически описания, като например в интерфейса за програмиране на приложения (API) или друга документация, предназначена за разработчици и други технически специалисти. При избора на продукти или услуги адвокатите трябва да използват надеждни източници на информация, включително проверени уебсайтове, уебсайтове на общности или дискусионни форуми, както и обратна връзка от други практикуващи адвокати.

Адвокатите трябва да анализират споразуменията за ниво на обслужване от гледна точка на тяхното изпълнение, сигурност, обработване на данни и защита на данните и да знаят, че съществуват три вида договори: просто спазване, договорени и смесени.

При това адвокатите трябва да обръщат специално внимание на следните аспекти на услугата:

- **Наличие и качество на поддръжка (обслужване на клиенти)** – колкото по-широк е обхватът на услугите, предоставяни от даден доставчик, толкова по-вероятно е ползвател адвокат да разчита на съдействие като клиент на този доставчик. В такъв случай наличието на отзивчиви служители, които

предоставят полезни съвети на клиентите на доставчика на ИТ е един от най-важните аспекти.

- **Финансова стабилност на доставчика и история на услугите** – проверете публикуваните финансови отчети и данните за дружеството в търговския регистър, колко дълго е съществувала тази структура на собственост и от колко време даденият доставчик предоставя услугите, които ще ползвате (напр. чрез интернет архивни услуги).
- **Наличие и качество на информацията за предоставяните услуги** – избраните доставчици трябва да разполагат с качествена информация за своите услуги, включително технически подробности (напр. доставчици на облачна инфраструктура или платформи, наричани съкратено IaaS и PaaS).
- **Прозрачност по отношение на използваните подизпълнители** – най-полезната информация обикновено е включена в условията за защита на данните при подизпълнителите. Физическото местоположение на съхранението на данните също обикновено се включва само в условията за защита на данните.
- **Спазване на съответни сертификати, доклади и кодекси за поведение от страна на доставчика** – би било полезно адвокатите да проверят тези документи, тъй като за тях може да е трудно да оценят по друг начин надеждността на техническите възможности на доставчика на услуги. Някои от кодексите за поведение са Регистърът на CSA[21], Кодексът за поведение в облака на ЕС[22] и Кодексът за поведение на SWIPO[23].
- **Идентичност на подизпълнителите** – когато не е възможно адвокатите да проверят съответствието с тези кодекси или сертификати, адвокатите трябва да се стремят да идентифицират:
    - подизпълнителите, които избраният от тях доставчик на облачни услуги ще използва; и
    - обхвата на услугите на тези подизпълнители.

  За някои подизпълнителите може да се прилагат съответни сертификати или кодекси, което също може да даде на адвоката известна сигурност. Важно е да се отбележи, че съответствието на подизпълнителя по отношение на някои части от цялостната услуга невинаги може да е от значение за адвоката.[24]

  Алтернативен и изискващ повече ресурси подход е адвокатите ръчно да проверят какви разпоредби от дадения кодекс за поведение присъстват в публикуваните общи условия на доставчика на облачни услуги. Дори частичното съответствие въз основа на публикуваните общи условия дава по-релевантна представа за доставчика на услуги, отколкото ако изобщо не се прави направи такава проверка. Ако публикуваните общи условия не обхващат такава

[21] CSA Star Registry: https://cloudsecurityalliance.org/star/registry
[22] EU Cloud Code of Conduct: https://eucoc.cloud/en/home
[23] Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services Version: 2020, Date: 08-07-2020, available at: https://swipo.eu/wp-content/uploads/2020/07/SWIPO-IaaS-Code-of-Conduct.pdf
[24] Това може да се случи, когато например доставчикът на ИТ услуги на адвоката ще може да прехвърли данните от своя доставчик подизпълнител към друг – и това не означава, че адвокатът ще може да прехвърли своите данни към друг доставчик.

информация, адвокатите трябва първо да се опитат да получат информация директно от доставчика или неговия дистрибутор по тези въпроси и да се стремят да включат всички уверения в сключените договорни условия.

- **Договорни условия** – когато няма технически решения, сертификати или кодекси за поведение, които да помогнат, адвокатите трябва да проверят и договорните условия на ИТ услугите за следната информация:
    - периодични резервни копия с високи нива на физическа и логическа сигурност;
    - механизми за автентикация за достъпа до информацията за адвокатите на адвокатската кантора и за клиентите;
    - криптиране на съхранени данни;
    - регистър на достъпа до данните;
    - одит на сигурността от надлежна трета страна;
    - използване на данните на потребителя от доставчика: данните на потребителя, качени или генерирани в облачна услуга, използвана от адвокат, не са предмет на никакво понятие за „собственост“ в ЕС и така доставчиците на ИТ като обработващи данни или притежатели на данни не следва да могат да претендират за никакви права във връзка с тези данни или да използват тези данни за цели, различни от тези, които са необходими само за предоставянето на услугата на адвоката. От друга страна, като се има предвид стойността на тези големи масиви от данни и трудността да се забележи подобна обработка, този риск остава реален. Понякога такава употреба може да се основава на анонимизирани данни, но анонимизацията рядко е трайно и сигурно решение, поради което може да доведе до значителни рискове, ако се извършва с данните на адвокатите. По тази причина адвокатите трябва да търсят ясни гаранции от доставчиците на услуги в техните условия, че няма да използват никакви данни на клиентите за цели, различни от предоставянето на услугата (независимо дали тези данни са лични или нелични).
    - Юрисдикция и решаване на спорове: Колкото и да е тривиално за адвокатите, все пак си струва да се отбележи, че дори и за тях може да е много трудно на практика да наложат правата, посочени в общите условия, ако съдилищата, компетентни по договора за услуги, са скъпи за съответния адвокат. Освен това много договори за SaaS предвиждат задължителен арбитраж или онлайн решаване на спорове, което рядко е от полза от гледна точка на малките адвокатски кантори, които търсят обезщетение.
    - Ограничаване на отговорността: Друг по-скоро тривиален момент, въз основа на който адвокатите могат лесно да сравняват различните доставчици на услуги, е ограничението на отговорността или по-скоро горната граница на преките вреди, които доставчикът на услуги се задължава да плати в случай на нарушение на договора. Подобно на повечето ИТ продукти, доставчиците на облачни услуги също

обикновено се опитват да ограничат собствената си отговорност, като изключват определени искове или категории вреди.

- Всякакви санкции или кредити за услуги в случай на неспазване на целите за ниво на обслужване: При сравняване на сходни услуги и доставчици следва да се даде предимство на тези, които са съгласни да предоставят поне символичен размер на неустойка или кредит за услуга, ако не изпълнят целите на нивото на обслужване (като например престой, време за реакция и др.).
- Срок и прекратяване на услугите: на последно място, преди да избере услуга, адвокатът трябва да разбере и как използваната услуга може да бъде прекратена както по негова собствена инициатива, така и по инициатива на доставчика. Условията трябва да включват процедура за възстановяване и миграция на данни за случай на прекратяване на договора. В допълнение, адвокатът трябва да изготви план за непрекъсваемост на дейността на адвокатската кантора в съответствие със сроковете за предизвестие за прекратяване на договора от страна на доставчика, както е посочено в договора. Това се отнася и за преносимостта на данните, при която адвокатите следва да могат да извличат данни в четим формат за по-нататъшна употреба или за целите на нормативното съответствие (напр. в областта на данъците).

7. Осведоменост за това къде се обработват данните

Адвокатите трябва да знаят къде и как се обработват данните на клиентите. Това включва проверка на правната и етичната допустимост на съхраняването на данни извън тяхната фирма, както и разбиране на разликите в законите за защита на данните в отделните юрисдикции и дали е разрешено прехвърлянето на данни извън ЕС и ако е разрешено, при какви условия. Ето защо адвокатите трябва да са наясно с механизмите за прехвърляне на данни, използвани от техните доставчици на облачни услуги, и с географските местоположения, които те използват за физическото съхранение на данните.

Механизми за предаване на данни

Съгласно ОРЗЩ са възможни няколко механизма за предаване на данни, описани в глава V:

- предаване въз основа на решение относно адекватното ниво на защита[25]
- предаване без решение относно адекватното ниво на защита.

[25] Списъкът с държави, обхванати от решенията за адекватното ниво на защита, е на разположение тук: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Ако няма решение за адекватност, следва да се използват други подходящи механизми за предаване на данни. Те включват задължителни фирмени правила, стандартни договорни клаузи, кодекси за поведение и схеми за сертифициране, дерогации съгласно член 49.[26]

- Стандартните договорни клаузи са примерен механизъм за предаване на данни, предназначен най-вече да помогне на администраторите и обработващите лични данни да улеснят законосъобразно предаването на данни към трети държави.
- Задължителните фирмени правила са правно обвързващи и приложими вътрешни правила и политики за предаване на данни в рамките на многонационални дружества от група.
- Кодексите за поведение са инструмент за предаване, разработен от асоциации, представляващи категории организации в даден сектор.
- Сертифицирането е нов инструмент за предаване на данни на организации, които са сертифицирани от сертифициращи органи или органи за защита на данните в ЕС/ЕИП. Този инструмент все още се разработва.
- Дерогациите по чл. 49 от ОРЗД позволяват предаването на данни в конкретни ситуации като напр. изпълнение на договор или защита на искове.

След решението по делото Schrems II Съдът на ЕС подчертава, че при предаването на лични данни извън ЕИП може да се наложи организациите да прилагат допълнителни мерки наред с подходящите предпазни мерки. Съдът на ЕС посочва, че администраторите или обработващите лични данни, когато действат като износители, трябва индивидуално да преценят дали законите или практиките на държавата извън ЕИП, като напр. тези, които налагат достъп до данни, не подкопават ефективността на гаранциите по чл. 46 от ОРЗД.

Предвид съображенията, изложени по-горе в настоящите насоки, адвокатите трябва да са наясно какви разпоредби се прилагат за данните, съхранявани от тяхната практика, и какви мерки трябва да предприемат, за да защитят материалите, попадащи в обхвата на правна професионална привилегия, професионалната тайна и съответните задължения за защита на данните.

На последно място, тъй като това е бързо развиваща се област и приложимите механизми за предаване на данни са били оспорвани в миналото, адвокатите трябва редовно да следят съответните актуализации на законодателството, съдебната практика и друга информация, за да бъдат в течение на своите задължения. Това включва, наред с друго, геополитическите дискусии относно сигурността на данните и потенциалната намеса на държавата като напр. „задни вратички“ или потоци от данни към държави, дори когато дружествата твърдят, че обработват техните данни в рамките на ЕС.

[26] EDPB guide on International data transfers

8. Осведоменост за това как се обработват данните

Предвид повсеместното разпространение на облачните услуги, адвокатите трябва да са наясно, че дори най-простите приложения и решения могат да включват обработка на данни от трети страни и по-нататъшно използване. Те могат да включват асистенти за редактиране на текст, превод, редактиране на изображения и др. Макар настоящите насоки да не разглеждат подробно тези услуги, адвокатите все пак трябва да са наясно с тези възможности за обработване на данни и свързаните с тях последици.

9. Съображения относно приемствеността на професионалната практика

Когато адвокатите съхраняват данни от разстояние, те трябва да се уверят, че данните могат да бъдат извлечени и че адвокатът продължава да контролира данните. За тази цел адвокатите следва да разполагат с подходящи механизми за непредвидени ситуации, които включват определяне на категориите данни, осигуряване на актуален местен достъп до критичните данни и наличие на алтернативна интернет връзка.

Дефиниране и категоризиране на критични данни

Данните трябва да се категоризират по важност и да се определи т.нар. цел на възстановяване (RPO): максималният период от време, който може да измине между бекъп на данни, преди загубата на данни да стане неприемлива от бизнес гледна точка. Това е решение, което трябва да бъде съзнателно взето от адвоката. За критични услуги в интерес на адвоката е да разбере дали могат да се правят локални резервни копия на данни от облачни услуги и ако да, как да се извършват такива локални резервни копия автоматично.

Определянето на критичните данни е нещо, което самите адвокати трябва да определят и разберат. То следва да обхваща данни, които (i) подлежат на задължения за съхранение от страна на адвоката и (ii) без които адвокатът може да не е в състояние да оказва ефективна помощ на клиента. Такова определение следва да вземе предвид конкретната услуга, предоставена на клиента, всички договорни обещания, дадени на клиента относно съхраняването на данните в споразумението за ангажимент, и рисковете за клиента при липса на такава непрекъсната правна услуга. При определянето на критични данни следва да се вземе предвид и фактът, че някои данни могат да бъдат възстановени от източници на трети страни (включително от съдебни документи или при повторно искане от клиентите да изпратят изгубени данни).

Осигуряване на актуален местен достъп до важни данни

Най-важният въпрос за адвоката е да разбере как да запази актуално локално копие на най-новите данни за клиента, с които разполага. Това би могло да включва работа с електронна поща по начин, който гарантира, че локалните копия (кешове) на

пощенските кутии са винаги на разположение (напр. използване на IMAP, POP, .OST или предложения на трети страни за най-големите доставчици на услуги за електронна поща). Предвид забележките относно поверителността по-горе, адвокатите трябва също така да обмислят дали тези доставчици от трети страни имат достъп до данните, които обработват.

Същият механизъм е необходим и за други хранилища на данни, които не са свързани със съобщения, като например настолни клиенти или локални сървъри, които автоматично се синхронизират с хранилището в облака. Само наличието на техническа възможност за изтегляне на всички такива данни не е достатъчно; адвокатите трябва да гарантират, че могат да разполагат с такова копие на критичните данни, като се вземе предвид приемливата за фирмата цел за точка на възстановяване. Съществува и риск изтриването на копия от едно устройство да доведе до изтриването им от други устройства, свързани със същата синхронизирана (споделена) система от папки. Този риск е по-висок, когато много потребители имат достъп до една и съща споделена папка.

Това е по-голям проблем, ако онлайн решенията за управление на практики или дела съхраняват такива критични данни. В сравнение с традиционните решения за съхранение в облак тези инструменти се продават за фрагментирани пазари със сравнително малко клиенти и дори най-популярните от тях може да не поддържат автоматизирани локални резервни копия от общото, като ще липсват и решения от трети страни. Това е допълнителен риск, който адвокатите също трябва да вземат под внимание.

От едно решение за управление на практиката не се очаква всички данни, съхранявани в тази система за управление на практиката, да са достъпни на местно ниво, но поне критичните данни трябва да са достъпни по начин, по който местните ИТ експерти могат технически да ги пресъздадат или да ги предоставят на адвокатите за по-нататъшно използване в малко вероятния случай на внезапна и постоянна недостъпност на доставчика на услуги. Обикновените обещания в договорните условия не могат да заменят техническата достъпност на критичните данни.

Алтернативен интернет достъп

Независимо от това колко се е увеличило използването на изчисления в облака, най-слабото звено от гледна точка на крайния потребител все още е достъпът до интернет от помещенията на адвокатската кантора. Благодарение на напредъка в електронните комуникации биха могли да бъдат налични алтернативни начини за достъп до интернет като например наличието на алтернативен доставчик на широколентов достъп (използващ различна от първоначалната разпределителна и опорна мрежа, а не просто препродавач на същите линии) или един или повече мобилни мрежови достъпа, към които адвокатската кантора (или автоматично всички устройства, които тя използва) може да превключи, когато е необходима резервна връзка. Адвокатите трябва да се

уверят, че разполагат с такава алтернативна организация, когато е необходимо, и да тестват подобни преходи поне веднъж годишно. В допълнение, за някои адвокатски кантори е препоръчително да помислят за резервен план в случай на по-общо спиране на електрозахранването или на интернет. Те трябва също така да обмислят възможността за запазване на критични данни на физически носител, който е изключен от интернет.

10. Осигуряване на подходящо застрахователно покритие

Тъй като адвокатите съхраняват чувствителни и поверителни данни на клиенти, те трябва да обмислят сключването на киберзастраховка, за да се предпазят от нежелани разходи за нарушаване на сигурността на данните, от разходи за възстановяване на дейността и от загуби на стопанската дейност в резултат на киберинцидент. В допълнение, адвокатите следва да преценят дали имат покритие за искове за вреди от трети лица в резултат на киберинциденти като например атаки с цел откуп, а също и за вреди в резултат на хардуерни проблеми (които често са изключени от стандартното покритие).

Адвокатите трябва също така да обмислят възможността да предвидят договорна клауза, която изисква от доставчика на облачни услуги да поддържа адекватна застраховка, която да покрива отговорността му по споразумението за облачни услуги.

III. Заключение

Изчисленията в облак са свързани с много рискове и проблеми, както е посочено в настоящите насоки, особено по отношение на поверителността/правната професионална привилегия и съхранението на данни. ССВЕ приканва адвокатските колегии и правните общества да повишават осведомеността на своите членове за по-голяма бдителност и да предприемат предпазни мерки на високо ниво. Правните и техническите предпазни мерки следва да им бъдат предоставени от техните доставчици на услуги за изчисления в облак (т.е. дългосрочна гаранция за бекъп на данните и др.).

Ето защо адвокатските колегии и правните общества се насърчават да подкрепят адвокатите по въпроси, свързани с използването на облачни услуги. Някои адвокатски колегии и правни общества могат дори да обмислят разработването на частни инфраструктури и услуги за изчисления в облак както за своите индивидуални, така и за колективните си членове в съответствие с горепосочените съображения. В такъв случай би било добре да извършат оценка на въздействието.[27]

[27] ССВЕ проучва и влиянието на изменението на климата върху адвокатите и тяхната практика. За тази цел ССВЕ разработва насоки в помощ на адвокатските колегии и правните общества, за да разгледат потенциалното въздействие на изменението на климата върху адвокатската практика, което може има отношение към използването на изчисления в облака.