Становище на Европейския надзорен орган по защита на данните (ЕНОЗД) относно Предложение за регламент на Европейския парламент и на Съвета относно Европейската агенция за мрежова и информационна сигурност (ENISA)

(2011/C 101/04)

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ,

като взе предвид Договора за функционирането на Европейския съюз и по-специално член 16 от него,

като взе предвид Хартата на основните права на Европейския съюз и по-специално член 7 и 8 от нея,

като взе предвид Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни ([1]),

като взе предвид искането за становище в съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни ([2]),

ПРИЕ НАСТОЯЩОТО СТАНОВИЩЕ:

I. ВЪВЕДЕНИЕ

Описание на предложението

1. На 30 септември 2010 г. Комисията прие предложение за регламент на Европейския парламент и на Съвета относно ENISA, Европейската агенция за мрежова и информационна сигурност ([3]).

2. ENISA е създадена през март 2004 г. за първоначален период от пет години с Регламент (ЕО) № 460/2004 ([4]). През 2008 г. мандатът ѝ беше удължен с Регламент (ЕО) № 1007/2008 ([5]) до март 2012 г.

3. Както следва от член 1, параграф 1 от Регламент (ЕО) № 460/2004, Агенцията е създадена с цел гарантиране на високо и ефективно ниво на мрежова и информационна сигурност в рамките на Съюза и допринасяне за безпрепятственото функциониране на вътрешния пазар.

4. Целта на предложението на Комисията е Агенцията да се модернизира, компетенциите ѝ да се укрепят и да се установи нов мандат за период от пет години, който ще позволи непрекъснатост на услугите ѝ след март 2012 г. ([6]).

5. Правното основание на предложения регламент се намира в член 114 от Договора за функционирането на Европейския съюз (ДФЕС) ([7]), с който на Съюза се предоставят правомощия да приема мерките, предназначени за установяване или осигуряване на функционирането на вътрешния пазар. Член 114 от ДФЕС замества член 95 от предишния договор за ЕО, на който са основани предишните регламенти за ENISA ([8]).

6. Обяснителният меморандум, придружаващ предложението, се отнася до факта, че предотвратяването и борбата с престъпността се превърнаха в съвместна компетенция на Съюза след влизането в сила на Договора от Лисабон. По този начин беше създадена възможността ENISA да служи като платформа за свързаните с МИС (мрежова и информационна сигурност) аспекти на борбата с кибернетичните престъпления, както и да обменя мнения и най-добри практики с органи за кибернетична отбрана, правоприлагане и защита на данните.

7. От няколко възможности Комисията избра да предложи увеличаване на задачите на ENISA и да включи правоприлагащите органи и органите за защита на данните като пълноправни членове на нейната група на заинтересовани страни. Новият списък със задачи не включва такива от оперативен характер, а актуализира и преформулира настоящите.

Консултация с ЕНОЗД

8. На 1 октомври 2010 г. предложението беше изпратено на ЕНОЗД за консултация в съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001. ЕНОЗД приветства факта, че към него се обръщат за становище по този въпрос, и препоръчва то да бъде упоменато в съображенията на предложението, подобно на редица други законодателни текстове, за които е била поискана консултация с ЕНОЗД в съответствие с Регламент (ЕО) № 45/2001.

9. Преди приемането на предложението с ЕНОЗД е проведена неофициална консултация и са получени няколко неофициални коментари. Въпреки това никоя от тези забележки не е взета под внимание в крайната версия на предложението.

Обща оценка

10. ЕНОЗД подчертава, че сигурността на обработването на данни е ключов елемент в защитата на данните ([9]). В това отношение той приветства целта на предложението да укрепи компетенциите на Агенцията, за да може тя

([1]) ОВ L 281, 23.11.1995 г., стр. 31.
([2]) ОВ L 8, 12.1.2001 г., стр. 1.
([3]) COM(2010) 521 окончателен.
([4]) ОВ L 77, 13.3.2004 г., стр. 1.
([5]) ОВ L 293, 31.10.2008 г., стр. 1.
([6]) За да предотврати правен вакуум, в случай че законодателната процедура в Европейския парламент и Съвета продължи след изтичане на текущия мандат, на 30 септември 2010 г. Комисията прие второ предложение за изменение на Регламент (ЕО) № 460/2004, с което се цели единствено да се удължи срока на настоящия мандат с 18 месеца. Вж. COM(2010) 520 окончателен.
([7]) Вж. по-горе.
([8]) На 2 май 2006 г. Съдът на Европейските общности отхвърли жалба за отмяна на предишния Регламент (ЕО) № 460/2004, която оспорваше неговото правно основание (дело C-217/04).
([9]) Изискванията за сигурност се съдържат в член 22 и 35 от Регламент (ЕО) № 45/2001, член 16 и 17 от Директива 95/46/ЕО и член 4 и 5 от Директива 2002/58/ЕО.

по-ефективно да изпълнява текущите си задачи и отговорности и едновременно с това да разшири своето поле на дейност. Освен това ЕНОЗД приветства включването на органите за защита на данните и правоприлагащите органи като пълноправни заинтересовани страни. Той смята, че удължаването на мандата на ENISA е начин на европейско равнище да се поощри професионално и стройно управление на мерките за сигурност на информационните системи.

11. Цялостната оценка на предложението е положителна. И все пак няколко точки от предложения регламент са неясни или непълни, което поражда загриженост от гледна точка на защитата на данни. Тези въпроси са обяснени и обсъдени в следващата глава от това становище.

II. **КОМЕНТАРИ И ПРЕПОРЪКИ**

Разширеният обхват на задачите, които ENISA ще извършва, не е достатъчно ясен

12. Разширеният обхват на задачите на Агенцията, свързани с участието на правоприлагащи органи и органи за защита на данните, е формулиран по много общ начин в член 3 от предложението. Обяснителният меморандум в това отношение е по-подробен. В него за ENISA е посочено, че тя взаимодейства с правоприлагащите органи при киберпрестъпленията и извършва задачи от неоперативен характер в борбата с киберпрестъпленията. И все пак тези задачи не са включени или само са споменати доста общо в член 3.

13. За да се избегне правна несигурност, предложеният регламент следва да е ясен и недвусмислен по отношение на задачите на ENISA. Както се споменава, сигурността на обработването на данни е ключов елемент от защитата на данни. ENISA ще има все по-важна роля в тази област. На гражданите, институциите и органите трябва да е ясно в какъв вид дейности е възможно ENISA да участва. Подобно измерение е дори още по-важно, в случай че разширеният обхват на задачите на ENISA включва обработването на лични данни (вж. точки 17—20 по-долу).

14. В член 3, параграф 1, буква к) от предложението е заявено, че Агенцията изпълнява всякакви други задачи, възложени на Агенцията по силата на друг законодателен акт на Съюза. ЕНОЗД изразява загриженост относно тази клауза с отворен край, тъй като тя създава потенциална възможност за заобикаляне, което може да повлияе на съгласуваността на правния инструмент и да доведе до „изместване на функциите“ на Агенцията.

15. Една от посочените задачи в член 3, параграф 1, буква к) от предложението, се съдържа в Директива 2002/58/ЕО ([1]). В него е предвидено, че от Комисията се изисква да предоставя консултация на Агенцията по всички технически мерки за изпълнение, приложими за изискванията за уведомяване в контекста на нарушения на сигурността на данни. ЕНОЗД препоръчва тази дейност на Агенцията да се опише по-подробно, така че границите ѝ да бъдат определени в областта на сигурността. Предвид потенциалното въздействие, което е възможно ENISA да окаже върху развитието на политиката в тази област, тази дейност следва да има по-ясна и по-видна позиция в рамките на предложения регламент.

16. Освен това ЕНОЗД препоръчва в съображение 21 да се включи препратка към Директива 1999/5/ЕО ([2]) предвид специалната задача на ENISA, посочена в член 3, параграф 1, буква в) от настоящото предложение, да съдейства държавите-членки и европейските институции и органи в усилията им за събиране, анализиране и разпространение на данни за мрежовата и информационна сигурност. Това следва да улесни рекламните дейности на ENISA в полза на най-добрите практики и техники на МИС (мрежова и информационна сигурност), тъй като ще спомогне за по-доброто илюстриране на възможните конструктивни взаимодействия между Агенцията и органите по стандартизация.

Следва да се изясни дали личните данни ще бъдат обработвани от Агенцията

17. В предложението не е уточнено дали е възможно възложените на Агенцията задачи да включват обработването на лични данни. Следователно предложението не съдържа специално правно основание за обработването на лични данни по смисъла на член 5 от Регламент (ЕО) № 45/2001.

18. Въпреки това някои от задачите, възложени на Агенцията, е възможно да включват (поне до определена степен) обработването на лични данни. Например не е изключено анализът на инциденти, свързани със сигурността, и нарушенията на сигурността на данните или извършването на функции от неоперативен характер в борбата с киберпрестъпленията, да включва събиране и анализ на лични данни.

19. Съображение 9 от предложението се отнася до разпоредбите в Директива 2002/21/ЕО ([3]), според които по целесъобразност Агенцията трябва да бъде уведомявана и от националните регулаторни органи в случай на нарушения, свързани със сигурността. ЕНОДЗ препоръчва предложението да включва повече подробности относно кои уведомления трябва да се изпратят на ENISA и относно начина, по който ENISA следва да им отговори. Също така предложението следва да включва последствията за обработването на лични данни, които могат да възникнат при анализа на тези уведомления (ако има такива).

([1]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) ОВ L 201, 31.7.2002 г., стр. 37.

([2]) Директива 1999/5/ЕО на Европейския парламент и на Съвета от 9 март 1999 година относно радионавигационното оборудване и далекосъобщителното крайно оборудване и взаимното признаване на тяхното съответствие, ОВ L 91, 7.4.1999 г., стр. 10, и по-специално член 3, параграф 3, буква в) от нея.

([3]) Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 година относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива, ОВ L 108, 24.4.2002 г., стр. 33).

20. ЕНОЗД приканва законодателя да изясни дали и ако това е така, кои дейности на ENISA, изброени в член 3, ще включват обработването на лични данни.

Следва да се уточнят правилата за вътрешна сигурност за ENISA

21. Въпреки че ENISA има важна роля в обсъждането на мрежовата и информационната сигурност в Европа, предложението почти не дава информация относно установяването на мерки за сигурност за самата Агенция (независимо дали са свързани с обработването на лични данни).

22. ЕНОЗД е на мнение, че Агенцията ще бъде дори в по-добра позиция да насърчава добрите практики във връзка със сигурността на обработването на данни, ако подобни мерки за сигурност цялостно се приложат вътрешно от самата Агенция. Това ще благоприятства признаването на Агенцията не само като център за експертни знания, но и като отправна точка в практическото прилагане на най-добрите налични техники (НДНТ) в областта на сигурността. Следователно стремежът към отлично качество в прилагането на практики в областта на сигурността следва да стане неразделна част от регламента, уреждащ процедурите за работа на Агенцията. Затова ЕНОЗД предлага в този смисъл към предложението да се добави разпоредба например, чрез която от Агенцията се изисква да прилага най-добрите налични техники, което означава най-ефективните и модерни процедури за сигурност и методите им на работа.

23. Този подход ще позволи на Агенцията да дава консултации относно практическата пригодност на конкретните техники на предоставяне на изискваните гаранции за сигурност. Освен това при прилагане на тези НДНТ приоритет следва да имат онези, които позволяват гарантиране на сигурността, като в същото време, доколкото е възможно, свеждат до минимум възможното въздействие върху личния живот. Следва да се избират техники, които съответстват повече на понятието „неприкосновеност на личния живот чрез проектното решение“.

24. Дори и при не толкова амбициозен проект, ЕНОЗД препоръчва регламентът да съдържа най-малко следните изисквания: i) създаване на политика на вътрешна сигурност в резултат на цялостна оценка на риска и вземане под внимание на международните стандарти и най-добрите практики в държавите-членки; ii) назначаване на служител по въпросите на сигурността, отговарящ за прилагане на политиката с подходящите ресурси и от подходящия орган; iii) одобряване на тази политика след внимателно изследване на остатъчния риск и проверките, предложени от управителния съвет; и iv) периодичен преглед на политиката, като избраната времева рамка на периодичността и целите на прегледа са ясно изложени.

Каналите на сътрудничество с органите за защита на данните (включително ЕНОЗД) и работната група по член 29, следва да са по-ясно дефинирани

25. Както вече беше заявено, ЕНОЗД приветства удължаването на мандата на Агенцията и вярва, че органите за защита на данните могат да извлекат значителна полза от съществуването ѝ (както и тя от експертните знания на тези органи). Имайки предвид естественото и логично сливане на сигурността и защитата на данни, Агенцията и органите за защита на данните наистина биват приканени да участват в тясно сътрудничество.

26. В съображения 24 и 25 е направена препратка към предложената директива на ЕС относно кибернетичните престъпления и в тях се споменава, че Агенцията следва да си сътрудничи с правоприлагащите органи и също органите за защита на данните във връзка с аспектите на борбата с кибернетичните престъпления, свързани с информационната сигурност ([1]).

27. Предложението следва да предоставя също конкретни канали и механизми на сътрудничество, които ще i) гарантират *съгласуваността* на дейностите на Агенцията с тези на органите за защита на данните; и ii) ще позволят *тясно сътрудничество* между Агенцията и органите за защита на данните.

28. По отношение на *съгласуваността* в съображение 27 изрично се прави препратка към факта, че задачите на Агенцията следва да не влизат в конфликт с органите за защита на данните на държавите-членки. ЕНОЗД приветства тази препратка, но отбелязва, че не е направена препратка към ЕНОЗД и работната група по член 29. ЕНОЗД препоръчва на законодателя също да включи в предложението сходна разпоредба за ненамеса във връзка с тези два субекта. Това ще спомогне създаването на по-ясна работна среда за всички страни и би следвало да оформи каналите и механизмите на сътрудничество, които ще позволят на Агенцията да съдейства различните органи за защита на данните и работната група по член 29.

29. Следователно, по отношение на *тясното сътрудничество* ЕНОЗД приветства включването на представителство на органите за защита на данните в Постоянната група на заинтересовани страни, която ще консултира Агенцията при изпълняване на дейностите ѝ. Той препоръчва изрично да се спомене, че подобно представителство от националните органи за защита на данните следва да се назначава от Агенцията въз основа на предложение от работната група по член 29. Също така би било добре, ако се включи препратка, която гарантира присъствието на ЕНОЗД, в качеството му на надзорен орган, на срещите, на които ще се обсъждат въпроси, свързани със сътрудничеството с ЕНОЗД. Освен това ЕНОЗД препоръчва Агенцията (консултирана от Постоянната група на заинтересовани страни и с одобрението на управителния съвет) да установи работни *ad hoc* групи за различните теми, по които защитата и сигурността на данните се припокриват, за да може Агенцията да придаде форма на това усилие за сътрудничество.

([1]) Предложение за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета, COM(2010) 517 окончателен.

30. И накрая, за да се избегне всякакво възможно недоразумение, ЕНОЗД препоръчва използването на „органи за защита на данни“, вместо „органи за защита на неприкосновеността на личния живот“ и изяснява кои са тези органи, като включва препратка към член 28 от Директива 95/46/ЕО ЕНОЗД, както е предвидено в Глава V от Регламент (ЕО) № 45/2001.

Не е ясно кои бенефициери могат да отправят искане за съдействие от ENISA

31. ЕНОЗД отбелязва несъответствие в предложения регламент във връзка с това кой може да отправи искане за съдействие от ENISA. От съображения 7, 15, 16, 18 и 36 от предложението следва, че ENISA има капацитета да съдейства на органите на държавите-членки и Съюза като цяло. Въпреки това член 2, параграф 1 се отнася само до Комисията и държавите-членки, докато с член 14 капацитетът да отправя искане за съдействие се ограничава до: i) Европейския парламент; ii) Съвета; iii) Комисията; и iv) всеки компетентен орган, назначен от държава-членка, с изключение на някои институции, органи, агенции и служби на Съюза.

32. Член 3 от предложението е по-специфичен и в него са представени различни видове съдействие в зависимост от типа бенефициери: i) събиране и анализиране на данни за мрежовата и информационна сигурност (в случай на държави-членки и европейските институции и органи); ii) анализиране състоянието на мрежовата и информационна сигурност в Европа (в случай на държави-членки и европейските институции и органи); iii) насърчаване използването на управление на риска и на добри практики (навсякъде в Съюза и държавите-членки); iv) развиване на способност за установяване на проблеми в сферата на мрежовата и информационна сигурност (в европейските институции и органи); и v) сътрудничеството в диалога и съвместната работа с трети страни (в случай на Съюза).

33. ЕНОДЗ приканва законодателя да поправи несъответствието и да уеднакви гореизложените разпоредби. В тази връзка ЕНОДЗ препоръчва член 14 да се измени по начин, който наистина включва всички институции, органи, служби и агенции на Съюза и който е ясен от гледна точка на съдействието, което различните субекти в Съюза могат да изискат (в случай че това ограничение е предвидено от законодателя). В същата насока се препоръчва определени обществени и частни субекти да могат да отправят искане за съдействие от Агенцията, ако при това съдействие е виден сигурен потенциал от европейска гледна точка то е в съответствие с целите на Агенцията.

Функции на управителния съвет

34. С обяснителния меморандум са предвидени компетенциите на управителния съвет във връзка с неговата надзорна роля. ЕНОДЗ приветства увеличените правомощия и препоръчва към функциите на управителния съвет да се включат няколко аспекта във връзка със защитата на данните. Освен това ЕНОДЗ препоръчва в регламента недвусмислено да се уточни кой има право да: i) установява мерки за прилагане на Регламент (ЕО) № 45/2001 от Агенцията, включително онези, свързани с назначаване на служител по защитата на данните; ii) одобрява политиката в областта на сигурността и последващите периодичните преразглеждания; и iii) изготвя протокола от сътрудничеството с органите за защита на данните и правоприлагащите органи.

Приложимост на Регламент (ЕО) № 45/2001

35. Въпреки че това вече се изисква съгласно Регламент (ЕО) № 45/2001, ЕНОДЗ предлага в член 27 да се включи назначаване на служител по защита на данните, тъй като това е от особено значение и следва да бъде придружено от своевременното поставяне на правила за прилагане във връзка с обхвата на правомощията и задачите, възлагани на служителя по защита на данните в съответствие с член 24, параграф 8 от Регламент (ЕО) № 45/2001. По-специално, член 27 би могъл да се чете, както следва:

1. Информацията, обработвана от Агенцията в съответствие с този регламент ще бъде предмет на Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 година относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни;

2. Управителният съвет ще установи мерки за приложението на Регламент (ЕО) № 45/2001 от страна на Агенцията, включително онези, свързани със служителя на по защита на данните на Агенцията.

36. В случай, че се изисква специално правно основание за обработването на лични данни, както бе посочено в точки 17—20 по-горе, то също следва да предвижда подробности относно необходимите и подходящите гаранции, ограничения и условия, при които ще се състои подобно обработване.

III. **ЗАКЛЮЧЕНИЯ**

37. Цялостната оценка на предложението е положителна и ЕНОДЗ приветства удължаването на мандата на Агенцията и разширяването на обхвата на задачите ѝ чрез включване на органи за защита на данните и правоприлагащи органи като пълноправни заинтересовани страни. ЕНОЗД счита, че непрекъснатостта на услугите на Агенцията ще насърчи на европейско равнище професионално и стройно управление на мерките за сигурност на информационните системи.

38. ЕНОДЗ препоръчва, че за да се избегне правна несигурност, предложението следва да се изясни във връзка с разширяването на обхвата на задачите на Агенцията и по-специално на онези, които са свързани с участието на правоприлагащи органи и органи за защита на данните. Също така ЕНОДЗ насочва вниманието към потенциалната възможност за заобикаляне, създадена с включването на разпоредба в предложението, която позволява добавяне на нови задачи за Агенцията посредством всеки друг законодателен акт на Съюза, без допълнително ограничение.

39. ЕНОДЗ приканва законодателя да изясни дали и ако това е така, кои дейности на ENISA ще включват обработването на лични данни.

40. ЕНОДЗ препоръчва включване на разпоредби относно установяването на политика в областта на сигурността на самата Агенция, за да укрепи ролята на Агенцията като двигател на отлично качество в прилагането на практики в областта на сигурността и като фактор за насърчаване на неприкосновеността на личния живот чрез проектното решение, интегрирайки използването на най-добрите налични техники в сигурността по отношение на правата на защита на личните данни.

41. Каналите за сътрудничество с органите за защита на данните, включително ЕНОДЗ и работната група по член 29, следва да се дефинират по-ясно с цел да се гарантира съгласуваност и тясно сътрудничество.

42. ЕНОДЗ приканва законодателя да разреши някои несъответствия във връзка с ограниченията, изразени в член 14, относно капацитета за отправяне на искане за съдействие от Агенцията. По-специално ЕНОДЗ препоръчва тези ограничения да се отнемат, а всички институции, органи, агенции и служби на Съюза да получат правомощия да отправят искане за съдействие от Агенцията.

43. И накрая, ЕНОДЗ препоръчва увеличените правомощия на управителния съвет да включват някои конкретни аспекти, които биха могли да подобрят достоверността, че добрите практики в Агенцията се следват във връзка със сигурността и защитата на данните. Наред с другото е направено предложение да се включи назначаването на служител по защита на данните и одобряване на мерките, насочени към правилното приложение на Регламент (ЕО) № 45/2001.

Съставено в Брюксел на 20 декември 2010 година.

Giovanni BUTTARELLI

Асистент към Европейския надзорен орган по защита на данните