Резюме на становището на Европейския надзорен орган по защита на данните относно Съвместно съобщение на Комисията и на Върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност за „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“ и за Директива относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза

(Пълният текст на настоящото становище може да бъде намерен на английски, френски и немски език на уебсайта на ЕНОЗД http://www.edps.europa.eu)

(2014/C 32/10)

1. **Въведение**

1.1. *Консултация с ЕНОЗД*

1. На 7 февруари 2013 г. Комисията и Върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност приеха Съвместно съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите за „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“ ([1]) (наричано по-долу „Съвместното съобщение“, „Стратегията за киберсигурност“ или „Стратегията“).

2. В същия ден Комисията прие предложение за Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза ([2]) (наричана по-долу „предложената Директива“). Това Предложение беше изпратено за консултация от ЕНОЗД на 7 февруари 2013 г.

3. Преди приемането на съвместното съобщение и на предложението, на ЕНОЗД беше предоставена възможност да отправи неофициални коментари. ЕНОЗД приветства факта, че много от тези коментари бяха взети предвид в съвместното съобщение и в предложението.

4. **Заключения**

74. ЕНОЗД приветства факта, че Комисията и Върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност представиха всеобхватна стратегия за киберсигурност, допълнена от директива за мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност (МИС) в ЕС. Стратегията допълва вече разработените действия на политиката в областта на мрежовата и информационната сигурност.

75. ЕНОЗД приветства факта, че стратегията надхвърля традиционния подход на противопоставяне между сигурността и правото на неприкосновеност на личния живот на физическите лица чрез гарантиране на изричното признаване на правото на неприкосновеност на личния живот и защита на данните като основни ценности, които следва да насочват политиката в областта на киберсигурността в ЕС и на международно равнище. ЕНОЗД отбелязва, че стратегията за киберсигурност и предложената Директива относно МИС може да имат основна роля в приноса за гарантиране на защитата на правата на неприкосновеност на личния живот на физическите лица и защитата на данните в онлайн пространството. В същото време трябва да се гарантира, че те няма да доведат до мерки, представляващи незаконна намеса в правата на физическите лица на неприкосновеност на личния живот и защита на данните.

76. ЕНОЗД също така приветства факта, че защитата на данните се посочва в няколко части от стратегията и е взета под внимание в предложената Директива относно МИС. Въпреки това той изразява съжаление, че в стратегията и в предложената директива не се подчертават по по-добър начин приносът на съществуващото и предстоящото законодателство в областта на защитата на данните, и за сигурността и невъзможността да се гарантира напълно, че всички задължения, произтичащи от предложената директива или други елементи от стратегията, са допълнителни към задълженията за защита на данните и не се припокриват или не си противоречат помежду си.

77. Освен това ЕНОЗД отбелязва, че поради липсата на обсъждане и пълно отчитане на други паралелни инициативи на Комисията и продължаващи законодателни процедури, като например реформата в областта на защитата на данните и предложеният регламент относно електронната идентификация и удостоверителните услуги, стратегията за киберсигурност не може да предостави изчерпателен и цялостен преглед на киберсигурността в ЕС и рискува да превърне фрагментирания и сегментиран подход в трайна тенденция. ЕНОЗД

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

също така отбелязва, че предложената директива относно МИС също все още не разрешава всеобхватен подход в областта на сигурността в ЕС, както и че задължението, заложено в законодателството в областта на защитата на данни, представлява вероятно най-всеобхватната рамка и задължение за сигурност съгласно законодателството на ЕС.

78. ЕНОЗД също така изразява съжаление, че важната роля на органите за защита на данните в изпълнението и прилагането на задълженията за сигурност и в подобряването на киберсигурността също не е надлежно отчетена.

79. Що се отнася до стратегията за киберсигурност, ЕНОЗД подчертава, че:

— ясното определение на термините „устойчивост на киберпространството“, „киберпрестъпност“ и „кибернетична отбрана“ е особено важно, тъй като тези термини се използват като обосновка за определени специални мерки, които могат да доведат до незаконна намеса в основни права, включително правата на неприкосновеност на личния живот и защита на данните. Въпреки това определенията за „киберпрестъпност“, предоставени в стратегията и в Конвенцията за престъпления в кибернетичното пространство, са твърде общи. Желателно е да се даде ясно и *ограничително* определение на „киберпрестъпност“ вместо подвеждащо такова;

— законодателството в областта на защитата на данните следва да се прилага за всички действия на стратегията винаги когато те се отнасят до мерки, предполагащи обработване на лични данни. Въпреки че законодателството в областта на защитата на данните не е специално посочено в разделите, свързани с киберпрестъпността и кибернетичната отбрана, ЕНОЗД подчертава, че много от действията, запланувани в тази област, включват обработването на лични данни и следователно попадат в обхвата на приложимото законодателство в областта на защитата на данните. Той също така отбелязва, че много действия се състоят от създаване на механизми за координация, което ще изисква прилагането на подходящи предпазни мерки за защита на данните относно условията за обмен на лични данни;

— органите за защита на данните (ОЗД) имат важна роля в контекста на киберсигурността. Като пазители на правата на неприкосновеност на личния живот и защита на данните на физическите лица, ОЗД участват активно в защитата на личните данни както офлайн, така и онлайн. Поради това те следва да имат подходящо участие в качеството си на надзорни органи с оглед на прилагането на мерки, които включват обработването на лични данни (като например стартирането на пилотния проект на ЕС за борба с т.нар. ботмрежи и зловредния софтуер). Други участници в областта на киберсигурността следва също така да си сътрудничат с тях в изпълнението на своите задачи, например в обмена на най-добри практики и действия за повишаване на осведомеността. ЕНОЗД и националните ОЗД следва също така да имат подходящо участие в конференцията на високо равнище, която ще се проведе през 2014 г. с цел оценка на напредъка по изпълнението на стратегията.

80. Що се отнася до предложената директива относно МИС, ЕНОЗД съветва законодателите да се:

— предостави повече яснота и сигурност в член 3, параграф 8 относно определението на участниците на пазара, които попадат в обхвата на Предложението, както и да се изготви изчерпателен списък, в който са включени всички съответни заинтересовани страни, с оглед на гарантирането на напълно хармонизиран и интегриран подход за сигурността в рамките на ЕС;

— поясни в член 1, параграф 2, буква в), че предложената Директива се прилага за всички институции и органи на ЕС, както и да се включи препратка към Регламент (ЕО) № 45/2001 в член 1, параграф 5 от Предложението;

— признае по-хоризонтална роля, която има настоящото предложение по отношение на сигурността, като изрично се посочи в член 1, че то следва да се прилага, без да засяга съществуващи или бъдещи по-подробни правила в специфични области (като например правилата, които предстои да бъдат установени относно доставчиците на удостоверителни услуги в предложения Регламент относно електронната идентификация);

— добави съображение, в което да се обясни необходимостта от утвърждаване на защитата на данните още при проектирането и по подразбиране в ранен етап от проектирането на механизмите, установени в Предложението, както и през целия жизнен цикъл на процеси, процедури, организации, техники и инфраструктури, като се вземе под внимание предложеният Регламент относно защитата на данните;

— пояснят определенията „мрежова и информационна система“ в член 3, параграф 1 и „инцидент“ в член 3, параграф 4, както и да се замени в член 5, параграф 2 задължението за създаване на „план за оценка на риска“ със „създаване и поддръжка на рамка за управление на риска“;

— уточни в член 1, параграф 6, че обработването на лични данни е обосновано съгласно член 7, буква д) от Директива 95/46/ЕО, дотолкова доколкото е необходимо за изпълнението на цели от обществен интерес, преследвани от предложената директива. Трябва обаче да се гарантира дължимото зачитане на принципите на необходимост и пропорционалност, за да се обработват единствено данните, абсолютно необходими за постигането на целите;

— изложат в член 14 обстоятелствата, при които се изисква уведомление, както и съдържанието и форматът на уведомлението, включително видовете лични данни, за които следва да се подаде уведомление, и дали и до каква степен уведомлението и придружаващите го документи ще включват детайли за лични данни, засегнати от конкретен инцидент, свързан със сигурността (като например IP адреси). Трябва да се вземе под внимание фактът, че компетентните органи в сферата на МИС следва да имат право да събират и обработват лични данни в рамките на инциденти, свързани със сигурността само тогава, когато това е абсолютно необходимо. В предложението следва също така да бъдат заложени подходящи предпазни мерки за гарантиране на надеждна защита на данните, обработвани от компетентните органи в сферата на МИС;

— поясни в член 14, че уведомленията за инциденти съгласно член 14, параграф 2 следва да се прилагат, без това да засяга задълженията за уведомление за нарушаване на сигурността на лични данни съгласно приложимото законодателство в областта на защитата на данни. В предложението следва да бъдат изложени основните аспекти на процедурата за сътрудничество на компетентните органи в сферата на МИС с ОЗД в случаите, когато инцидентът, свързан със сигурността, включва нарушаване на сигурността на личните данни;

— измени член 14, параграф 8 така, че изключването на микропредприятията от обхвата на уведомленията да не е приложимо за тези оператори, които имат основна роля в предоставянето на услуги на информационното общество, например с оглед на характера на информацията, която те обработват (напр. биометрични данни или чувствителни данни);

— добавят разпоредби в Предложението за уреждане на допълнителния обмен на лични данни между компетентните органи в сферата на МИС и други получатели, за да се гарантира, че i) личните данни се разкриват само на получатели, които е необходимо да ги обработват за изпълнението на своите задачи в съответствие с подходящо правно основание, и ii) тази информация е ограничена само до необходимото за изпълнението на тези задачи. Следва също така да се вземе под внимание това как организациите, предоставящи данни на мрежата за обмен на информация, гарантират съответствие с принципа за ограничаване в рамките на целта;

— посочи срокът за съхранение на лични данни за целите, изложени в предложената Директива, по-специално по отношение на съхранението от компетентните органи в сферата на МИС и в рамките на сигурната система за обмен на информация;

— напомни на компетентните органи в сферата на МИС за задължението им да предоставят подходяща информация на субектите на данните относно обработването на лични данни, например чрез публикуването на политика за поверителност на своя уебсайт;

— добави разпоредба във връзка с нивото на сигурност, което трябва да бъде спазвано от компетентните органи в сферата на МИС във връзка с информацията, която подлежи на събиране, обработване и обмен. По отношение на защитата на лични данни от компетентните органи в сферата на МИС следва бъде включена специална препратка към изискванията за сигурност на член 17 от Директива 95/46/ЕО;

— поясни в член 9, параграф 2, че критериите за участие на държавите членки в сигурната система за обмен на информация следва да гарантират, че всички участници в системите за споделяне на информация осигуряват високо ниво на сигурност и устойчивост във всички етапи от обработването. Тези критерии следва да включват подходящи мерки за поверителност и сигурност в съответствие с членове 16 и 17 от Директива 95/46/ЕО и членове 21 и 22 от Регламент (ЕО) № 45/2001. Комисията следва да бъде изрично обвързана с тези критерии поради участието си като администратор в сигурната система за обмен на информация;

— добави в член 9 описание на ролите и отговорностите на Комисията и на държавите членки в изготвянето, експлоатирането и поддръжката на сигурната система за обмен на информация, както и да се гарантира, че проектирането на системата следва да се извърши в съответствие с принципите за защитата на данните още при проектирането и по подразбиране и за сигурност още при проектирането; и

— добави в член 13, че всяко прехвърляне на лични данни към получатели, намиращи се в държави извън ЕС, следва да се осъществява в съответствие с членове 25 и 26 от Директива 95/46/ЕО и член 9 от Регламент (ЕО) № 45/2001.

Съставено в Брюксел на 14 юни 2013 година.

Peter HUSTINX

Европейски надзорен орган по защита на данните