II

(Nem jogalkotási aktusok)

RENDELETEK

A BIZOTTSÁG 1179/2011/EU VÉGREHAJTÁSI RENDELETE

(2011. november 17.)

az online gyűjtési rendszerekre vonatkozó technikai előírásoknak a polgári kezdeményezésről szóló 211/2011/EU európai parlamenti és tanácsi rendelet értelmében történő megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a polgári kezdeményezésről szóló, 2011. február 16-i 211/2011/EU európai parlamenti és tanácsi rendeletre [1] és különösen annak 6. cikke (5) bekezdésére,

az európai adatvédelmi biztossal folytatott konzultációt követően,

mivel:

(1) A 211/2011/EU rendelet előírja, hogy amennyiben a támogató nyilatkozatokat online gyűjtik, az e célból alkalmazott rendszernek meg kell felelnie bizonyos biztonsági és műszaki követelményeknek, és azt az érintett tagállam illetékes hatóságának kell igazolnia.

(2) Az online gyűjtési rendszer a 211/2011/EU rendelet értelmében olyan információs rendszer, amely szoftverből, hardverből, üzemeltetési környezetből, üzleti folyamatokból és személyzetből áll a támogatási nyilatkozatok online gyűjtésének elvégzése céljából.

(3) A 211/2011/EU rendelet előírja azokat a követelményeket, amelyeknek az online gyűjtési rendszereknek az igazoláshoz meg kell felelniük, és meghatározza, hogy a Bizottságnak technikai előírásokat kell elfogadnia e követelmények végrehajtása céljából.

(4) Az OWASP (Open Web Application Security Project) Top 10 2010 projektje áttekintést ad a webes alkalmazások legjelentősebb biztonsági kockázatairól, valamint eszközöket nyújt ezen kockázatok kezelésére; a technikai előírások ezért e projekt megállapításaira támaszkodnak.

(5) A technikai előírások szervezők általi végrehajtásának garantálnia kell, hogy a tagállamok hatóságai igazolják az online gyűjtési rendszereket, és hozzá kell járulnia, a megfelelő technikai és szervezési intézkedések végrehajtásának biztosításához a 95/46/EK európai parlamenti és tanácsi irányelv [2] által meghatározott kötelezettségeknek való megfeleléshez, a biztonság fenntartása, és ezáltal az engedély nélküli adatfeldolgozás megelőzése érdekében mind az adatfeldolgozó rendszer megtervezésekor, mind az adatfeldolgozás időpontjában, valamint hogy megvédjék a személyes adatokat a véletlen megsemmisüléstől vagy jogellenes megsemmisítéstől vagy véletlen elvesztéstől, megváltoztatástól, jogosulatlan nyilvánosságra hozataltól vagy hozzáféréstől.

(6) Az igazolási folyamatot célszerű elősegíteni annak előírásával, hogy a szervezők a Bizottság által a 211/2011/EU rendelet 6. cikke (2) bekezdésének megfelelően rendelkezésre bocsátott szoftvert használják.

(7) A polgári kezdeményezés szervezőinek – adatkezelői minőségükben, a támogató nyilatkozatok online gyűjtésekor – végre kell hajtaniuk az e rendeletben meghatározott technikai előírásokat a feldolgozott személyes adatok védelmének biztosítása érdekében. Amennyiben az adatokat egy adatfeldolgozó dolgozza fel, a szervezőknek biztosítaniuk kell, hogy az adatfeldolgozó kizárólag a szervezőktől kapott utasítások alapján jár el és végrehajtja az e rendeletben meghatározott technikai előírásokat.

(8) Ez a rendelet tiszteletben tartja az alapvető jogokat és betartja az Európai Unió Alapjogi Chartájában foglalt elveket, különös tekintettel az Alapjogi Charta 8. cikkére, amely értelmében mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

(9) Az e rendeletben előírt intézkedések összhangban vannak a 211/2011/EU rendelet 20. cikke által létrehozott bizottság véleményével,

[1] HL L 65., 2011.3.11., 1. o.

[2] HL L 281., 1995.11.23., 31. o.

ELFOGADTA EZT A RENDELETET:

1. cikk

A 211/2011/EU rendelet 6. cikkének (5) bekezdésében említett technikai előírásokat a melléklet tartalmazza.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2011. november 17-én.

a Bizottság részéről
az elnök
José Manuel BARROSO

MELLÉKLET

1. A 211/2011/EU RENDELET 6. CIKKE (4) BEKEZDÉSE a) PONTJÁNAK VÉGREHAJTÁSÁT CÉLZÓ TECHNIKAI ELŐÍRÁSOK

Annak érdekében, hogy a rendszerben ne kerülhessen sor a támogató nyilatkozatok automatizált benyújtására, az aláírónak a támogató nyilatkozat benyújtása előtt át kell esnie az aktuális gyakorlatnak megfelelő célirányos ellenőrzésen. Az ellenőrzés történhet például egy erős „captcha" (karakterfelismerő teszt) használatával.

2. A 211/2011/EU RENDELET 6. CIKKE (4) BEKEZDÉSE b) PONTJÁNAK VÉGREHAJTÁSÁT CÉLZÓ TECHNIKAI ELŐÍRÁSOK

Információvédelmi szabványok

2.1. A szervezők dokumentációval bizonyítják, hogy megfelelnek az ISO/IEC 27001 szabvány követelményeinek, az annak elfogadására vonatkozó követelmény kivételével. Ebből a célból, a szervezők:

a) olyan teljes körű kockázatértékelést végeztek, amely: azonosítja a rendszer hatókörét; bemutatja, hogy az információvédelem különböző sérülései milyen hatást gyakorolhatnak a végzett tevékenységre; felsorolja az információs rendszert érintő fenyegetéseket és a rendszer biztonsági réseit; kockázatelemzési dokumentumot eredményez, amely tartalmazza egyrészt az ilyen fenyegetésekkel kapcsolatos óvintézkedéseket, valamint a fenyegetések esetleges megvalósulása esetén teendő intézkedéseket és végül fontossági sorrendben felsorolja az elvégzendő javításokat;

b) megtervezték és végrehajtották a kockázatok kezelésére vonatkozó intézkedéseket a személyes adatok védelmére, valamint a családi és magánélet védelmére tekintettel, valamint azokat az intézkedéseket, amelyeket a kockázatos események bekövetkezése esetén hoznak meg;

c) írásban azonosították a fennmaradó kockázatokat;

d) szervezési eszközöket biztosítottak az új fenyegetésekre és biztonsági fejlesztésekre vonatkozó visszajelzések fogadása érdekében.

2.2. A szervezők biztonsági ellenőrzéseket választanak a 2.1. a) pontban található kockázatelemzés alapján a következő szabványokból:

1. ISO/IEC 27002; vagy

2. az Információbiztonsági Fórum által kidolgozott „bevált gyakorlatok szabványa" (Standard of Good Practice vagy SoGP),

a következő kérdések kezelésére:

a) kockázatértékelések (javasolt az ISO/IEC 27005 vagy egyéb konkrét és megfelelő kockázatértékelési módszertan);

b) fizikai és környezeti biztonság;

c) humánerőforrás-biztonság;

d) kommunikáció- és műveletirányítás;

e) a hozzáférés-vezérlésre vonatkozó szabványos intézkedések, az e végrehajtási rendeletben meghatározott intézkedéseken felül;

f) információs rendszerek beszerzése, fejlesztése és fenntartása;

g) információbiztonsági kezelés;

h) intézkedések az információs rendszerek olyan rendszerbiztonsági eseményeinek orvoslására és csökkentésére, amelyek a feldolgozott személyes adatoknak megsemmisítését vagy véletlen elvesztését, megváltoztatását, jogosulatlan nyilvánosságra hozatalát vagy az ahhoz való jogosulatlan hozzáférést eredményeznék;

i) megfelelés (Compliance);

j) a számítógépes hálózat biztonsága (javasolt az ISO/IEC 27033 vagy a bevált gyakorlatok szabványa (SoGP)).

A szabványok alkalmazását elegendő csak a szervezet online gyűjtés szempontjából releváns részei számára előírni. A humánerőforrás-biztonság például lekorlátozható a személyzet azon részére, amelynek fizikai vagy hálózati hozzáférése van az online gyűjtési rendszerhez, a fizikai/környezeti biztonság pedig a rendszernek otthont adó épület(ek)re korlátozható le.

Funkcionális követelmények

2.3. Az online gyűjtési rendszer egy webalapú alkalmazásból áll, amelyet egy bizonyos polgári kezdeményezésre vonatkozó támogató nyilatkozatok gyűjtésére hoztak létre.

2.4. Amennyiben a rendszer üzemeltetése különböző feladatköröket tesz szükségessé, úgy ezekhez különböző hozzáférési szinteket kell létrehozni a minimális üzemeltetési jogosultság (a lehető legkevesebb jogosultság) elvének megfelelően.

2.5. A nyilvánosan elérhető funkciókat egyértelműen el kell választani a rendszer üzemeltetésére szánt funkcióktól. A hozzáférés-vezérlés nem akadályozhatja a rendszer nyilvános területén rendelkezésre álló információk olvasását, beleértve a kezdeményezésre vonatkozó információt és a támogató nyilatkozat elektronikus formanyomtatványát. A kezdeményezés aláírása kizárólag e nyilvános területen keresztül lehetséges.

2.6. A rendszer észleli és megakadályozza a támogató nyilatkozatok kettőzött benyújtását.

Az alkalmazási szint biztonsága

2.7. A rendszer megfelelően védett az ismert biztonsági rések és az azok elleni „exploit” típusú támadások ellen. Ebből a célból többek között a következő követelményeknek tesz eleget:

2.7.1. A rendszer védelmet nyújt az olyan kódbeszúrásos támadások (injections) ellen, mint a strukturált lekérdezési nyelv (Structured Query Language, SQL) alapján történő lekérdezések, a könnyű címtár elérési protokoll (Lightweight Directory Access Protocol, LDAP) alapján történő lekérdezések, az XML Path nyelv (XPath) alapján történő lekérdezések, az operációs rendszerparancsok vagy programargumentumok. Ebből a célból alapkövetelmény, hogy:

a) valamennyi felhasználó által megadott bemenő paramétereket ellenőrzik;

b) az ellenőrzés legalább a szerveroldali logikán keresztül történjen;

c) valamennyi értelmezőprogram egyértelműen válassza szét a nem megbízható adatokat a parancstól vagy lekérdezéstől. Az SQL-hívásokra vonatkozóan ez azt jelenti, hogy kötési változókat (bind variables) használnak valamennyi kidolgozott utasításban (prepared statements) és tárolt eljárásban (stored procedures), valamint elkerülik a dinamikus lekérdezéseket.

2.7.2. A rendszer védelmet nyújt a honlap közti parancsfájlt alkalmazó támadások (Cross-Site Scripting, XSS) ellen. Ebből a célból alapkövetelmény, hogy:

a) ellenőrizzék minden, a böngészőre visszaküldött felhasználói input biztonságosságát (a bemenő paraméterek ellenőrzése útján);

b) valamennyi felhasználói inputot megfelelően kódolnak (escape), mielőtt megjelenik az output oldalon;

c) az output megfelelő kódolása biztosítja, hogy az ilyen inputot mindig szövegként kezelik a böngészőben, és nem használnak semmilyen aktív tartalmat.

2.7.3. A rendszer szigorú hitelesítéssel és munkamenet-kezeléssel rendelkezik, amely szerint alapkövetelmény, hogy:

a) a hitelesítő adatok a tárolás idején mindig védelem alatt állnak kivonatolással (hashing) vagy titkosítással. Csökken annak kockázata, hogy valaki „pass-the-hash” támadást alkalmazva hitelesít;

b) a hitelesítő adatokat nem lehet kitalálni vagy felülírni gyenge fiókkezelési funkciók révén (pl. fiók létrehozása, jelszó módosítása, jelszó helyreállítása, gyenge munkamenet-azonosítók (session ID-k));

c) a munkamenet (session) azonosítói és a munkamenetadatok nem jelennek meg az URL-n (Uniform Resource Locator);

d) a munkamenet azonosítóit nem veszélyeztetik a munkamenet-rögzítéses támadások;

e) a munkamenet-azonosítók korlátozott idejűek, ami biztosítja, hogy a felhasználók ne maradjanak bejelentkezve;

f) a munkamenet-azonosítókat sikeres bejelentkezés után nem használják fel újra;

g) jelszavakat, munkamenet-azonosítókat és egyéb hitelesítő adatokat csak TLS protokollon (Transport Layer Security) keresztül küldenek meg;

h) a rendszer adminisztrációs része is védelem alatt áll. Amennyiben egytényezős hitelesítés (Single-factor Authentication, SFA) védi, akkor a jelszónak minimum tíz karakterből kell állnia, beleértve legalább egy betűt, egy számot és egy speciális karaktert. Választási lehetőségként a kéttényezőjű hitelesítést is használhatják. Amennyiben csak egytényezős hitelesítést használnak, az magában foglalja a rendszer adminisztrációs részéhez interneten való hozzáférésre vonatkozó kétlépcsős ellenőrzési mechanizmust, amelyben az egy tényezőt bővítik a hitelesítés egyéb eszközeivel, mint az egyszeri kódszó/SMS-n keresztüli kód vagy egy aszimmetrikusan titkosított véletlenszerű karakterláncra épülő jelkód (Challenge String), amelyet a szervezők/rendszeradminisztrátorok rendszer számára ismeretlen személyes kulcsával kell megfejteni.

2.7.4. A rendszer nem rendelkezik nem biztonságos közvetlen objektumhivatkozással. Ebből a célból alapkövetelmény, hogy:

a) a korlátozott erőforrásokra való közvetlen hivatkozásokra vonatkozóan, az alkalmazás ellenőrzi, hogy a felhasználó jogosult-e a kért erőforráshoz való hozzáférésre;

b) amennyiben a hivatkozás közvetett hivatkozás, a közvetett hivatkozáshoz való hozzárendelés az aktuális felhasználó számára engedélyezett értékekre korlátozódik.

2.7.5. A rendszer védelmet nyújt a honlap közti lekérdezésekkel kapcsolatos manipulációk (Cross-Site Request Forgery, XSRF) ellen.

2.7.6. Megfelelő biztonsági konfigurációt hoztak létre, amely szerint alapkövetelmény, hogy:

a) valamennyi szoftverösszetevő naprakész legyen, beleértve az operációs rendszert, a webalkalmazás-kiszolgálót, az adatbázis-kezelő rendszert (DBMS), az alkalmazásokat, valamint valamennyi kódkönyvtárat;

b) az operációs rendszer és a web/alkalmazás kiszolgáló szükségtelen szolgáltatásai le vannak tiltva, el vannak távolítva vagy nincsenek telepítve;

c) a fiók alapértelmezett jelszavait megváltoztatták vagy letiltották;

d) a hibakezelés kialakítása megakadályozza, hogy a veremkivonatokon és egyéb túlságosan informatív hibaüzeneteken keresztül érzékeny információk szivárogjanak ki;

e) a fejlesztési keretekben és könyvtárak biztonsági beállításai olyan bevált gyakorlatoknak megfelelően vannak konfigurálva, mint az OWASP iránymutatásai.

2.7.7. A rendszer az alábbiak szerint rendelkezik az adatok titkosításáról:

a) a személyes adatokat elektronikus formában akkor titkosítják, amikor tárolják vagy átadják azokat a tagállamok illetékes hatóságainak a 211/2011/EU rendelet 8. cikkének (1) bekezdésével összhangban; a kulcsok kezelése és biztonsági mentése egymástól elválasztva történik;

b) szigorú standard algoritmusokat és szigorú kulcsokat alkalmaznak a nemzetközi szabványokkal összhangban. A kulcskezelés működik;

c) a jelszavakat kivonatolják szigorú szabvány algoritmusokkal és megfelelő „salt”-ot használnak;

d) valamennyi kulcsot és jelszót védik a jogosulatlan hozzáféréstől.

2.7.8. A rendszer felhasználói hozzáférési szintek és engedélyek révén korlátozza az URL-elérést. Ebből a célból alapkövetelmény, hogy:

a) amennyiben külső biztonsági mechanizmusokat alkalmaznak az oldalhoz való hozzáférésre vonatkozó hitelesítés és jogosultsági ellenőrzések nyújtására, azokat minden oldal esetében megfelelően kell konfigurálni;

b) amennyiben kódszintű védelmet alkalmaznak, a kódszintű védelemnek működnie kell minden egyes kért oldalra vonatkozóan.

2.7.9. A rendszer átvételi rétegének védelme (Transport Layer Protection) elegendő. Ebből a célból a következő intézkedések mindegyike vagy legalább azonos erősségű intézkedések vannak érvényben:

a) a rendszer a HTTPS (Hypertext Transfer Protocol Secure) legaktuálisabb verzióját igényli, hogy hozzáférjen valamennyi szenzitív erőforráshoz olyan hitelesítéseket alkalmazva, amelyek érvényesek, nem jártak le, nincsenek visszavonva és amelyek a webhely által használt valamennyi tartománnyal megegyeznek;

b) a rendszer minden szenzitív cookie-t „biztonságos” (secure flag) jelöléssel lát el;

c) a szerver úgy konfigurálja a TLS-szolgáltatót, hogy az csak a bevált gyakorlatoknak megfelelően titkosított algoritmusokat támogassa. A felhasználókat tájékoztatják, hogy engedélyezniük kell a TLS-támogatást a böngészőjükben.

2.7.10. A rendszer védelmet nyújt az érvénytelenített átirányítások és továbbítások ellen.

Adatbázis-biztonság és adatsértetlenség

2.8. Amennyiben a különböző polgári kezdeményezéseknél használt online gyűjtési rendszerek erőforrásokat osztanak meg a hardverre és az operációs rendszerekre vonatkozóan, azok nem osztanak meg adatokat, beleértve a hozzáférési/titkosítási hitelesítő adatokat. Ezt tükrözi ezen felül a kockázatértékelés és a végrehajtott ellenintézkedések.

2.9. Csökken annak kockázata, hogy valaki „pass-the-hash" támadás útján hozzáfér az adatbázishoz.

2.10. Az aláírók által szolgáltatott adatok csak az adatbázis kezelője/szervezője számára hozzáférhetőek.

2.11. A rendszeradminisztrátor hitelesítő adatai, az aláíróktól begyűjtött személyes adatok és azok biztonsági másolata szigorú titkosított algoritmusok által védett a 2.7.7. b) ponttal összhangban. A rendszerben azonban titkosítás nélkül tárolható a tagállam, ahol a támogató nyilatkozatot számításba veszik, a támogató nyilatkozat benyújtásának időpontja, és a nyelv, amelyen az aláíró a támogató nyilatkozat formanyomtatványát kitöltötte.

2.12. Az aláíróknak csak az azon munkamenet során benyújtott adatokhoz van hozzáférésük, amelyben a támogató nyilatkozat formanyomtatványát kitöltötték. Mihelyst a támogató nyilatkozat formanyomtatványát benyújtják, a fent említett munkamenet lezárul és a benyújtott adatok többé nem hozzáférhetőek.

2.13. Az aláírók személyes adatai csak a rendszerben állnak rendelkezésre, beleértve a biztonsági másolatot titkosított formátumban. A 211/2011/EU rendelet 8. cikkével összhangban a nemzeti hatóságoknak az adatokba való betekintés vagy azok igazolása érdekében, a szervezők a titkosított adatokat a 2.7.7. a) pontnak megfelelően exportálhatják.

2.14. A támogató nyilatkozat formanyomtatványába bevitt adatok megőrzése oszthatatlan (atomic). Ezért, mihelyst a felhasználó valamennyi szükséges részletet bevitte a támogató nyilatkozat formanyomtatványába és érvényesíti a kezdeményezés támogatásáról szóló döntését, a rendszer vagy sikeresen véglegesíti az összes űrlapadatot az adatbázisban, hiba esetén pedig egyáltalán nem ment el egyetlen adatot sem. A rendszer tájékoztatja a felhasználót, hogy kérése sikeres vagy sikertelen volt.

2.15. A használt adatbázis-kezelő rendszer (DBMS) naprakész, és folyamatosan javítják az újonnan felfedezett biztonsági rések kihasználása ellen.

2.16. A rendszer valamennyi műveleti naplója a helyén van. A rendszer biztosítja, hogy az alább felsorolt kivételeket és más biztonsággal kapcsolatos eseményeket rögzítő naplófájlokat készíthetnek és azokat megtarthatják, ameddig az adatokat a 211/2011/EU rendelet 12. cikk (3) és (5) bekezdéseivel összhangban meg nem semmisítik. A naplók megfelelő védelem alatt állnak, például titkosított adathordozón való tárolás útján. A szervezők/rendszeradminisztrátorok rendszeresen ellenőrzik a naplókat gyanús tevékenységekkel kapcsolatosan. A naplók tartalmazzák legalább:

a) a szervezők/rendszeradminisztrátorok bejelentkezésére és kijelentkezésére vonatkozó dátumot és időt;

b) az elvégzett biztonsági mentéseket;

c) az adatbázis rendszeradminisztrátorának valamennyi módosítását és frissítését.

Infrastruktúra-biztonság – fizikai hely, hálózati infrastruktúra és szerver környezet

2.17. *Fizikai biztonság*

Akármilyen típusú szerverhostingot használnak is, az alkalmazást üzemeltető gép megfelelően védett, amely az alábbiakat követeli meg:

a) a hosting területéhez való hozzáférés ellenőrzése és naplófájl;

b) a biztonsági másolat adatainak fizikai védelme lopás vagy véletlen adatvesztés ellen;

c) az alkalmazást üzemeltető szervert biztonságosan zárható rackszekrénybe telepítették.

2.18. *Hálózatbiztonság*

2.18.1. A rendszert egy internettel összekötött szerver működteti, amelyet ütközőzónában telepítettek és tűzfallal védett.

2.18.2. Amennyiben a tűzfal legfontosabb frissítései és javításai nyilvánosak lesznek, úgy az ilyen frissítéseket és javításokat ennek megfelelően telepítik.

2.18.3. A szerveren bemenő és kimenő összes forgalmat (amelyet az online gyűjtési rendszernek szánnak) megvizsgálják és naplózzák a tűzfalszabályoknak megfelelően. A tűzfalszabályok megtagadnak minden olyan forgalmat, amely nem szükséges a rendszer biztonságos használatával és üzemeltetésével kapcsolatosan.

2.18.4. Az online gyűjtési rendszert egy megfelelően védett termelési hálózati szegmensnek kell üzemeltetnie, amely el van választva az olyan szegmensektől, amelyek a nem termelő rendszereket üzemeltetik, mint a fejlesztési és tesztkörnyezetek.

2.18.5. A helyi hálózat (LAN) következő biztonsági intézkedései vannak érvényben:

a) Layer 2 (L2) hozzáférési listája/Kapcsolóport-biztonság;

b) a használaton kívüli kapcsolóportok le vannak tiltva;

c) az ütközőzóna egy kijelölt virtuális helyi hálózaton (VLAN)/helyi hálózaton (LAN) található;

d) nincs engedélyezett L2 trunk kapcsolat (L2 trunking) a felesleges portokon.

2.19. *Operációs rendszer és web/alkalmazás szerver biztonsága*

2.19.1. Megfelelő biztonsági konfigurációt hoztak létre, beleértve a 2.7.6. pontban felsorolt elemeket.

2.19.2. Az alkalmazások a futtatáshoz szükséges jogosultságok legalacsonyabb szintjével futnak.

2.19.3. A rendszeradminisztrátor hozzáférése az online gyűjtési rendszer kezelési felületéhez rövid, korlátozott időtartamú (a munkamenet maximum 15 perc).

2.19.4. Amennyiben az operációs rendszer, az alkalmazás futtatórendszerei, a szervereken futtatott alkalmazások vagy kártevőirtók legfontosabb frissítései és javításai nyilvánosak lesznek, úgy az ilyen frissítéseket és javításokat ennek megfelelően telepítik.

2.19.5. Csökken annak kockázata, hogy valaki „pass-the-hash" támadás útján hitelesíti a rendszert.

2.20. *A szervező ügyfélbiztonsága*

A végpontok közötti adatbiztonság érdekében a szervezők meghozzák a szükséges intézkedéseket, hogy biztonságossá tegyék azon ügyfélalkalmazásukat/eszközüket, amelyet az online gyűjtési rendszer kezelésére és ahhoz való hozzáféréshez használnak, mint például:

2.20.1. A felhasználók a nem karbantartásra vonatkozó feladatokat (mint az irodai automatizálási feladatok) a futtatáshoz szükséges jogosultságok legalacsonyabb szintjével futtatják.

2.20.2. Amennyiben az operációs rendszer, bármely telepített alkalmazás vagy vírusirtó legfontosabb frissítései és javításai nyilvánosak lesznek, úgy az ilyen frissítéseket és javításokat ennek megfelelően telepítik.

3. A 211/2011/EU RENDELET 6. CIKKE (4) BEKEZDÉSE c) PONTJÁNAK VÉGRAHAJTÁSÁT CÉLZÓ TECHNIKAI ELŐÍRÁSOK

3.1. A rendszer biztosítja annak lehetőségét mindegyik tagállam részére, hogy kivonatoljanak egy jelentést, amely felsorolja a kezdeményezést és az aláírók személyes adatait, amelyet az adott tagállam illetékes hatóságai ellenőriznek.

3.2. Az aláírók támogatási nyilatkozatainak exportálása a 211/2011/EU rendelet III. mellékletében található formanyomtatványban lehetséges. A rendszer ezen felül biztosítja a támogatási nyilatkozatok exportjának lehetőségét egy olyan interoperábilis formátumban, mint az XML (Extensible Markup Language).

3.3. Az exportált támogató nyilatkozatokat *korlátozott terjesztésűként* jelölik meg az érintett tagállam felé és *személyes adatként* sorolják be.

3.4. Az exportált adatok tagállamok felé történő elektronikus továbbítása védve van a lehallgatás ellen, a végpontok közötti megfelelő titkosítás használatával.