РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2015/1502 НА КОМИСИЯТА

от 8 септември 2015 година

за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО ([1]), и по-специално член 8, параграф 3 от него,

като има предвид, че:

(1) Съгласно член 8 от Регламент (ЕС) № 910/2014 за всяка схема за електронна идентификация, за която е извършено уведомяване съгласно член 9, параграф 1, (наричана по-долу „нотифицирана схема"), трябва да се определят нива на осигуреност „ниско", „значително" и „високо" за средствата за електронна идентификация, издадени по тази схема.

(2) Определянето на минималните технически спецификации, стандарти и процедури е от съществено значение, за да се гарантира общоприето разбиране на данните за нивата на осигуреност, както и да се гарантира оперативната съвместимост при категоризирането на националните нива на осигуреност на нотифицираните схеми за електронна идентификация спрямо нивата на осигуреност съгласно член 8, както е предвидено в член 12, параграф 4, буква б) от Регламент (ЕС) № 910/2014.

(3) Спецификациите и процедурите, посочени в настоящия акт за изпълнение, са съобразени с международния стандарт ISO/IEC 29115, тъй като той е основният международен стандарт в областта на нивата на осигуреност за средствата за електронна идентификация. Съдържанието на Регламент (ЕС) № 910/2014 обаче се различава от този международен стандарт, по-специално по отношение на изискванията за доказване и проверка на самоличността, както и в начина, по който са взети под внимание различията между разпоредбите на държавите членки за самоличността и съществуващите инструменти в ЕС за същата цел. Поради това приложението следва да се основава на този международен стандарт, но без позоваване към конкретно съдържание на ISO/IEC 29115.

(4) Настоящият регламент беше разработен по основан на резултатите подход като най-подходящ за целта, което се отразява и в определенията за термини и понятия. Те са съобразени с целта на Регламент (ЕС) № 910/2014 по отношение на нивата на осигуреност на средствата за електронна идентификация. Поради това широкомащабният пилотен проект STORK, включително разработените по него спецификации, както и определенията и понятията в ISO/IEC 29115, следва да бъдат взети под особено внимание при установяването на спецификациите и процедурите, посочени в настоящия акт за изпълнение.

(5) В зависимост от контекста, в който трябва да бъде проверен даден аспект на доказателството за самоличността, достоверните източници могат да са в множество различни форми, включително регистри, документи и органи. Достоверните източници могат да се различават в зависимост от държавата членка дори в сходен контекст.

(6) Изискванията за доказване и проверка на самоличността следва да са съобразени с различните системи и практики, като същевременно се гарантира достатъчно висока осигуреност, за да се установи необходимото доверие. Поради това приемането на процедури, използвани преди за цел, различна от издаването на средства за електронна идентификация, следва да бъде обвързано с условия за потвърждение, че тези процедури отговарят на изискванията, предвидени за съответното ниво на осигуреност.

([1]) ОВ L 257, 28.8.2014 г., стр. 73.

(7) Обикновено за удостоверяване на автентичността се използват някои фактори като споделени тайни, физически устройства и физически характеристики. Следва да се насърчава обаче използването на по-голям брой фактори за удостоверяване на автентичността — особено на фактори от различни категории, за да да се повиши сигурността на процеса на удостоверяване на автентичността.

(8) Настоящият регламент не следва да засяга правата за представителство на юридически лица. Въпреки това в приложението следва да са предвидени изисквания за обвързването между средствата за електронна идентификация на физически и юридически лица.

(9) Следва да се отчете значението на системите за информационна сигурност и за управление на услуги, както и важността на използването на общоприети методики и на прилагането на принципите, заложени в стандарти като ISO/IEC 27000 и тези от серията ISO/IEC 20000.

(10) Добрите практики във връзка с нивата на осигуреност в държавите членки също следва да бъдат взети предвид.

(11) Сертифицирането на сигурността на информационните технологии (ИТ) на базата на международни стандарти е важен инструмент за проверка на това дали по отношение на сигурността продуктите отговарят на изискванията на настоящия акт за изпълнение.

(12) Комитетът, посочен в член 48 от Регламент (ЕС) № 910/2014, не е представил становище в срока, определен от неговия председател,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

1. Нивата на осигуреност „ниско“, „значително“ и „високо“ за средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация, се определят с позоваване на спецификациите и процедурите, посочени в приложението.

2. Спецификациите и процедурите, посочени в приложението, се използват за установяване на нивото на осигуреност на средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация, като се определят надеждността и качеството на следните елементи:

а) вписването, както е посочено в раздел 2.1 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, буква а) от Регламент (ЕС) № 910/2014;

б) управлението на средствата за електронна идентификация, както е посочено в раздел 2.2 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, букви б) и е) от Регламент (ЕС) № 910/2014;

в) удостоверяването на автентичността, както е посочено в раздел 2.3 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, буква в) от Регламент (ЕС) № 910/2014;

г) управлението и организацията, както е посочено в раздел 2.4 от приложението към настоящия регламент, в съответствие с член 8, параграф 3, букви г) и д) от Регламент (ЕС) № 910/2014.

3. Когато средството за електронна идентификация, издадено по нотифицирана схема за електронна идентификация, отговаря на изискване, посочено за по-високо ниво на осигуреност, тогава се счита, че средството изпълнява равностойното изискване за по-ниско ниво на осигуреност.

4. Освен ако е указано друго в съответната част на приложението, за съответствие със заявеното ниво на осигуреност трябва да са налице всички елементи, изброени в приложението за определено ниво на осигуреност на средствата за електронна идентификация, издадени по нотифицирана схема за електронна идентификация.

Член 2

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 8 септември 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

Технически спецификации и процедури за нивата на осигуреност „ниско“, „значително“ и „високо“ за средства за електронна идентификация, издадени по нотифицирана схема за електронна идентификация

1. **Приложими определения**

За целите на наістоящото приложение се прилагат следните определения:

1) „достоверен източник“ означава който и да е източник, независимо от неговата форма, на който може да се разчита за получаването на точни данни, информация и/или факти, които могат да бъдат използвани, за да се докаже самоличността;

2) „фактор за удостоверяване на автентичността“ означава фактор, потвърден като свързан с дадено лице, който попада в една от следните категории:

   а) „фактор въз основа на притежание“ означава фактор за удостоверяване на автентичността, когато от субекта се изисква да докаже притежанието си върху него;

   б) „фактор въз основа на познаване“ означава фактор за удостоверяване на автентичността, когато от субекта се изисква да докаже познаването му;

   в) „присъщ фактор за удостоверяване на автентичността“ означава фактор, който се основава на физически атрибут на физическо лице и от субекта се изисква да докаже, че притежава този физически атрибут;

3) „динамично удостоверяване на автентичността“ означава електронен процес, при който се използва криптография или друга техника, която осигурява начин за създаване по заявка на електронно потвърждение, че субектът контролира или притежава данните за идентификация, и който се променя с всяко удостоверяване на автентичността между субекта и системата, проверяваща самоличността на субекта;

4) „система за управление на информационната сигурност“ означава набор от процеси и процедури, предназначени за управление до приемливи нива на рисковете, свързани с информационната сигурност.

2. **Технически спецификации и процедури**

Елементите на техническите спецификации и процедури, описани в настоящото приложение, се използват, за да се определи по какъв начин изискванията и критериите съгласно член 8 от Регламент (ЕС) № 910/2014 да се прилагат за средствата за електронна идентификация, издадени по схема за електронна идентификация.

2.1. *Вписване*

2.1.1. Заявяване и регистриране

Ниво на осигуреност	Необходими елементи
Ниско	1. Уверяване, че заявителят е запознат с реда и условията във връзка с използването на средствата за електронна идентификация. 2. Уверяване, че заявителят е запознат с препоръчаните предпазни мерки за сигурност във връзка със средствата за електронна идентификация. 3. Събиране на съответните данни за самоличност, изисквани за доказване и проверка на самоличността.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.1.2. Доказване и проверка на самоличността (физическо лице)

Ниво на осигуреност	Необходими елементи
Ниско	1. Може да се приеме, че лицето разполага с доказателство, което е признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност. 2. Доказателството може да се приеме за неподправено или за съществуващо съгласно достоверен източник и изглежда да е валидно. 3. От достоверен източник е известно, че заявената самоличност съществува, и може да се приеме, че лицето, което претендира за тази самоличност, съвпада с нея.
Значително	Трябва да бъдат изпълнени изискванията за нивото „ниско“, плюс една от алтернативите, изброени в точки 1—4: 1. Лицето е било проверено, че разполага с доказателство, което е признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност; както и доказателството се проверява, за да се определи дали е неподправено; или, съгласно достоверен източник, е известно, че съществува и се отнася за действително лице; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на лицето да не съответства на заявената самоличност, като се отчита например рискът доказателството да е загубено, откраднато, с прекратена валидност, отменено или с изтекъл срок; или 2. По време на процеса на регистрация е представен документ за самоличност, издаден в същата държава членка, и документът изглежда се отнася за представилото го лице; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на лицето да не съответства на заявената самоличност, като се отчита например рискът документът да е загубен, откраднат, с прекратена валидност, отменен или с изтекъл срок; или 3. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.2 за нивото „значително“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета [1], или от равностоен орган; или 4. Когато средствата за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „значително“ или „високо“, като се вземат под внимание рисковете от промяна в данните за идентификация на лицето, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „значително“ или „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган.

Ниво на осигуреност	Необходими елементи
Високо	Трябва да бъдат изпълнени изискванията или на точка 1, или на точка 2: 1. Трябва да бъдат изпълнени изискванията за нивото „значително“ плюс една от алтернативите, изброени в букви от а) до в): а) Когато лицето е проверено, че притежава снимково или биометрично доказателство за идентификация, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, и удостоверява заявената самоличност, доказателството се проверява, за да се установи дали то е валидно според достоверен източник; както и заявителят е идентифициран със заявената самоличност чрез сравняване на една или повече физически характеристики на лицето с достоверен източник; или б) Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.2 за нивото „високо“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; както и са предприети стъпки, за да се покаже, че резултатите от по-ранните процедури остават валидни; или в) Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „високо“, като се вземат под внимание рисковете от промяна в данните за идентификация на лицето, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; както и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура на издаване на нотифицирано средство за електронна идентификация остават валидни. ИЛИ 2. Когато заявителят не представи признато снимково или биометрично доказателство за идентификация, за получаване на такова признато снимково или биометрично доказателство за идентификация се прилагат абсолютно същите процедури, използвани на национално равнище в държавата членка на субекта, отговорен за регистрацията.

([1]) Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (ОВ L 218, 13.8.2008 г., стр. 30).

2.1.3. Доказване и проверка на самоличността (юридическо лице)

Ниво на осигуреност	Необходими елементи
Ниско	1. За заявената самоличност на юридическото лице се показва доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация.

Ниво на осигуреност	Необходими елементи
	2. Доказателството изглежда валидно и може да се приеме, че е неподправено или съществуващо съгласно достоверен източник, когато включването на юридическо лице в достоверния източник е доброволно и се урежда чрез договореност между юридическото лице и достоверния източник. 3. Не е известно от достоверен източник юридическото лице да се намира в състояние, което би го възпрепятствало да действа в това си качество.
Значително	Трябва да бъдат изпълнени изискванията за нивото „ниско“, плюс една от алтернативите, изброени в точки 1—3: 1. За заявената самоличност на юридическото лице се показва доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, включващо наименованието на юридическото лице, правната му форма и (ако е приложимо) неговия регистрационен номер; и доказателството се проверява, за да се определи дали то е неподправено или е известно като съществуващо съгласно достоверен източник, когато за дейността на юридическото лице в съответния сектор се изисква включването му в достоверния източник; както и са били предприети стъпки, за да се сведе до минимум рискът самоличността на юридическото лице да не съответства на заявената самоличност, като се отчита например рискът съответните документи да са загубени, откраднати, с прекратена валидност, отменени или с изтекъл срок; или 2. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.3 за нивото „значително“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; или 3. Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „значително“ или „високо“, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „значително“ или „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган.
Високо	Трябва да бъдат изпълнени изискванията за нивото „значително“, плюс една от алтернативите, изброени в точки 1—3: 1. За заявената самоличност на юридическото лице се представя доказателство, признато от държавата членка, в която се подава заявлението за средство за електронна идентификация, включващо наименованието на юридическото лице, правната му форма и най-малко един уникален идентификатор, представляващ юридическото лице и използван в национален контекст; и доказателството се проверява, за да се определи дали то е валидно съгласно достоверен източник; или

Ниво на осигуреност	Необходими елементи
	2. Когато процедурите, използвани преди това от публичноправен или частноправен субект в същата държава членка за цел, различна от издаването на средства за електронна идентификация, предоставят осигуреност, която е равностойна на посочената в раздел 2.1.3 за нивото „високо“, тогава не е необходимо субектът, отговорен за регистрацията, да повтаря тези предходни процедури, при условие че такава равностойна осигуреност е потвърдена от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура остават валидни; или 3. Когато средства за електронна идентификация се издават на основание валидно нотифицирано средство за електронна идентификация с ниво на осигуреност „високо“, не се изисква да се повтарят процесите на доказване и проверка на самоличността. Когато служещите за основание средства за електронна идентификация не са били нотифицирани, нивото на осигуреност „високо“ трябва да бъде потвърдено от орган за оценяване на съответствието, посочен в член 2, точка 13 от Регламент (ЕО) № 765/2008, или от равностоен орган; и са предприети стъпки, за да се покаже, че резултатите от тази предходна процедура на издаване на нотифицирано средство за електронна идентификация остават валидни.

2.1.4. Свързване между средствата за електронна идентификация на физически и на юридически лица

Когато е приложимо, за свързването между средствата за електронна идентификация на физическо лице и средствата за електронна идентификация на юридическо лице (наричано по-долу „свързването“) са в сила следните условия:

1) Трябва да е възможно да се прекрати временно и/или отмени свързването. Жизненият цикъл на свързването (например активиране, временно спиране, подновяване, отмяна) се управлява съгласно национално признати процедури.

2) Физическото лице, чието средство за електронна идентификация е свързано със средство за електронна идентификация на юридическото лице, може да делегира упражняването на свързването с друго физическо лице въз основа на национално признати процедури. Делегиращото физическо лице обаче продължава да носи отговорността.

3) Свързването се извършва по следния начин:

Ниво на осигуреност	Необходими елементи
Ниско	1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „ниско“ или по-високо. 2. Свързването е било осъществено въз основа на национално признати процедури. 3. Не е известно от достоверен източник физическото лице да се намира в състояние, което би го възпрепятствало да действа от името на юридическото лице.
Значително	Като точка 3 за ниво „ниско“, плюс: 1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „значително“ или „високо“.

Ниво на осигуреност	Необходими елементи
	2. Свързването е било осъществено въз основа на национално признати процедури, което е довело до регистриране на свързването в достоверен източник. 3. Свързването е било проверено въз основа на информация от достоверен източник.
Високо	Като точка 3 за ниво „ниско“ и точка 2 за ниво „значително“, плюс: 1. Проверява се дали доказването на самоличността на физическото лице, действащо от името на юридическото лице, е било извършено на ниво „високо“. 2. Свързването е било проверено въз основа на уникален идентификатор, представляващ юридическото лице и използван в националния контекст; и въз основа на информация от достоверен източник, представляваща по уникален начин физическото лице.

2.2. *Управление на средствата за електронна идентификация*

2.2.1. Характеристики и структура на средствата за електронна идентификация

Ниво на осигуреност	Необходими елементи
Ниско	1. При средството за електронна идентификация се използва най-малко един фактор за удостоверяване на автентичността. 2. Средството за електронна идентификация се проектира така, че издателят да предприема подходящи мерки, за да проверява, че то се използва само под контрола или във притежанието на лицето, на което принадлежи.
Значително	1. При средството за електронна идентификация се използват най-малко два фактора от различни категории за удостоверяване на автентичността. 2. Средството за електронна идентификация се проектира така, че да може да се приеме, че то се използва само под контрола или във притежанието на лицето, на което принадлежи.
Високо	Както за ниво „значително“, плюс: 1. Средството за електронна идентификация защитава срещу дублиране и подправяне, както и срещу нападатели с голям потенциал за атаки. 2. Средството за електронна идентификация е проектирано така, че лицето, на което принадлежи, да може да го защити надеждно срещу използване от други лица.

2.2.2. Издаване, предоставяне и активиране

Ниво на осигуреност	Необходими елементи
Ниско	След издаването му средството за електронна идентификация се предоставя по начин, за който може да се приеме, че гарантира получаване единствено от лицето, за което е предназначено.
Значително	След издаването на средството за електронна идентификация то се предоставя по начин, за който може да се приеме, че гарантира получаване единствено от лицето, на което принадлежи.
Високо	В процеса на активиране се проверява дали средството за електронна идентификация е било получено единствено от лицето, на което принадлежи.

2.2.3. Временно спиране на действието, отнемане и повторно активиране

Ниво на осигуреност	Необходими елементи
Ниско	1. Възможно е по своевременен и ефективен начин да се прекрати временно действието на дадено средство за електронна идентификация и/или то да се отнеме. 2. Наличието на мерки, предприети за предотвратяване на неразрешено временно спиране на действието, отнемане и/или повторно активиране. 3. Повторно активиране се извършва само ако продължава спазването на същите изисквания за осигуреност, както установените преди временното спиране на действието или отнемането.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.2.4. Подновяване и замяна

Ниво на осигуреност	Необходими елементи
Ниско	Като се вземат предвид рисковете от промяна в данните за идентификация на лицето, подновяването или замяната трябва да отговарят на същите изисквания за осигуреност, както първоначалното доказване и проверка на самоличността, или да се основава на валидно средство за електронна идентификация със същото или по-високо ниво на осигуреност.
Значително	Същите, както за нивото „ниско“.
Високо	Както за ниво „ниско“, плюс: Когато подновяването или замяната се основава на валидно средство за електронна идентификация, данните за самоличността се проверяват чрез достоверен източник.

2.3. *Удостоверяване на автентичността*

Настоящият раздел е посветен на заплахите, свързани с използването на механизма за удостоверяване на автентичността, и се изброяват изискванията за всяко ниво на осигуреност. За контролните мерки по настоящия раздел се подразбира, че те трябва да бъдат съизмерими с рисковете за даденото ниво.

2.3.1. Механизъм за удостоверяване на автентичността

В таблицата по-долу са посочени изискванията за отделните нива на осигуреност по отношение на механизма за удостоверяване на автентичността, чрез който физическото или юридическото лице използва средството за електронна идентификация, за да потвърди своята самоличност пред доверяваща се страна.

Ниво на осигуреност	Необходими елементи
Ниско	1. Разкриването на данни за идентификацията на лицето се предхожда от надеждна проверка на средството за електронна идентификация и неговата валидност. 2. Когато данните за идентификация на лица се съхраняват като част от механизма за удостоверяване на автентичността, тази информация се защитава срещу загуба и срещу компрометиране, включително анализ офлайн. 3. Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с повишен базов потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.

Ниво на осигуреност	Необходими елементи
Значително	Както за ниво „ниско“, плюс: 1. Разкриването на данни за идентификацията на лицето се предхожда от надеждна проверка на средството за електронна идентификация и неговата валидност чрез динамично удостоверяване на автентичността. 2. Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с умерен потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.
Високо	Както за ниво „значително“, плюс: Механизмът за удостоверяване на автентичността осъществява контролни мерки за сигурност за проверката на средството за електронна идентификация, така че е много малко вероятно нападател с голям потенциал за атака да може чрез дейности като налучкване, подслушване, възпроизвеждане или манипулиране на комуникацията да злоупотреби с механизма за удостоверяване на автентичността.

2.4. *Управление и организация*

Всички участници, предоставящи услуга, свързани с електронната идентификация в трансграничен контекст (наричани по-долу „доставчици“), трябва да разполагат с документирани практики и политики за управление на информационната сигурност, подходи за управление на риска и други признати контролни мерки, така че да предоставят гаранции пред компетентните органи по управление за схеми за електронна идентификация в съответните държави членки, че са налице ефективни практики. За всички изисквания/елементи в целия раздел 2.4 се подразбира, че те трябва да бъдат съизмерими с рисковете за даденото ниво.

2.4.1. Общи разпоредби

Ниво на осигуреност	Необходими елементи
Ниско	1. Доставчикът, предоставящ оперативна услуга, попадаща в обхвата на настоящия регламент, е държавен орган или правен субект, признат като такъв от националното право на държава членка, с установена организация и дейност във всички области, които имат отношение към предоставянето на услугата. 2. Доставчиците спазват всички правни изисквания, приложими за тях, във връзка с изпълнението и предоставянето на услугата, включително по отношение на видовете информация, в които може да се търси, как се извършва доказването на самоличността, каква информация може да бъде запазена и за какъв период от време. 3. Доставчиците са в състояние да докажат способността си да поемат риска от възникване на отговорност за причинени щети, както и да притежават достатъчно финансови ресурси за непрекъснато изпълнение и предоставяне на услугите. 4. Доставчиците носят отговорност за изпълнението на всички задължения, възложени на друг субект, и за спазването на политиката за схемата, все едно че те самите са изпълнявали задълженията. 5. За схемите за електронна идентификация, които не са учредени съгласно националното право, трябва да е налице ефективен план за прекратяването им. Такъв план трябва да включва надлежно прекратяване на услугата или продължаване от друг доставчик; начина, по който се информират за това съответните органи и крайните потребители, както и подробности относно начина, по който записите следва да бъдат защитени, запазени и унищожени в съответствие с политиката за схемата.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.2. Публикувани известия и информация за потребителите

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на публикувано определение за услугата, което включва всички приложими условия, ред и такси, както и всички ограничения за нейното използване. Определението за услугата трябва да включва политика за защита на правото на личен живот. 2. Трябва да бъдат въведени подходяща политика и процедури, за да се гарантира, че ползвателите на услугата са информирани по своевременен и надежден начин за всяка промяна в определението за посочената услуга и във всички приложими условия, ред и политика за защита на личния живот във връзка с тази услуга. 3. Трябва да бъдат въведени подходяща политика и процедури, които да осигуряват пълни и правилни отговори на исканията за информация.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.3. Управление на информационната сигурност

Ниво на осигуреност	Необходими елементи
Ниско	За управлението и контрола на рисковете, свързани със сигурността на информацията, съществува ефективна система за управление на информационната сигурност.
Значително	Както за ниво „ниско“, плюс: Системата за управление на информационната сигурност е съобразена с изпитани стандарти или принципи за управление и контрол на рисковете, свързани със сигурността на информацията.
Високо	Същите, както за нивото „значително“.

2.4.4. Водене на отчетност

Ниво на осигуреност	Необходими елементи
Ниско	1. Записване и съхраняване на значима информация посредством ефективна система за управление на записите, като се вземат предвид приложимото законодателство и добрите практики по отношение на защитата и запазването на данните. 2. Запазване, доколкото това е разрешено от националното законодателство или други национални административни разпоредби, и защита на записите за срок, съобразен с нуждите на одита, разследването на пробиви в сигурността и съхранението на данни, след което записите се унищожават по сигурен начин.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.5. Съоръжения и персонал

В следващата таблица са посочени изискванията по отношение на съоръженията и персонала и, ако е приложимо, подизпълнителите, които поемат задължения, обхванати от настоящия регламент. Спазването на всяко от изискванията трябва да е пропорционално на степента на рисковете, свързани с предоставяното ниво на осигуреност.

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на процедури, с които се гарантира, че персоналът и подизпълнителите са достатъчно обучени, квалифицирани и опитни за уменията, необходими за изпълнението на своите роли. 2. Наличието на достатъчен персонал и подизпълнители за адекватно изпълнение и поддържане на услугата съгласно политиките и процедурите за нея. 3. Съоръженията, използвани за предоставянето на услугата, са под непрекъснато наблюдение за предпазване от щети, причинени от екологични инциденти, неразрешен достъп и други фактори, които могат да повлияят на сигурността на услугата. 4. Съоръженията, използвани за предоставянето на услугата, осигуряват ограничаването до оправомощени служители или подизпълнители на достъпа до зоните за съхранение или обработка на лична, криптографска или друга чувствителна информация.
Значително	Същите, както за нивото „ниско“.
Високо	Същите, както за нивото „ниско“.

2.4.6. Технически проверки

Ниво на осигуреност	Необходими елементи
Ниско	1. Наличието на пропорционални технически проверки за управление на рисковете за сигурността на услугите с цел с цел защита на обработваната информация по отношение на нейната поверителност, цялостност и разполагаемост. 2. Електронните канали за комуникация, които се използват за обмен на лична или чувствителна информация, са защитени срещу подслушване, манипулиране и възпроизвеждане. 3. Достъпът до чувствителен криптографски материал, ако се използва такъв за издаване на средства за електронна идентификация и за удостоверяване на автентичност, е ограничен до роли и приложения, за които този достъп е абсолютно необходим. Трябва да се гарантира, че такъв материал никога не се съхранява продължително време като некодиран текст. 4. Съществуват процедури, за да се гарантира постоянно поддържане на сигурността, а също е налице способност да се реагира на промени в нивата на риска, инциденти и пробиви в сигурността. 5. Всички носители, съдържащи лична, криптографска или друга чувствителна информация, се съхраняват, транспортират и унищожават по сигурен и безопасен начин.
Значително	Същите, както за нивото „ниско“, плюс: Ако за издаване на средства за електронна идентификация и за удостоверяване на автентичност се използва чувствителен криптографски материал, той е защитен срещу подправяне.
Високо	Същите, както за нивото „значително“.

2.4.7. Спазване и одит

Ниво на осигуреност	Необходими елементи
Ниско	Наличие на периодични вътрешни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика.

Ниво на осигуреност	Необходими елементи
Значително	Наличие на периодични независими вътрешни или външни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика.
Високо	1. Наличие на периодични независими външни одити, обхващащи всички части, които са от значение за предоставянето на услугите, за да се гарантира спазването на съответната политика. 2. Когато дадена схема се управлява пряко от държавен орган, одитът за нея се извършва в съответствие с националното законодателство.