EBA/GL/2014/12_Rev1

19 декември 2014 г.

Окончателни насоки

относно сигурността на плащанията в интернет

Съдържание

Насоки относно сигурността на плащанията в интернет

Статут на настоящите насоки

Настоящият документ съдържа насоки, изготвени съгласно член 16 от Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията („Регламент за ЕБО“). Съгласно член 16, параграф 3 от Регламента за ЕБО компетентните органи и финансовите институции полагат всички усилия за изпълнение на насоките.

В насоките е представено становището на ЕБО за подходящите надзорни практики в Европейската система за финансов надзор или за това, как правото на Съюза следва да се прилага в дадена област. Поради това ЕБО очаква всички компетентни органи и финансови институции, за които са предназначени насоките, да ги спазват. Компетентните органи, за които се прилагат насоките, следва да ги спазват, чрез включването им в надзорните си практики както е уместно (напр. чрез изменение на тяхната правна рамка или надзорни процеси), включително в случаите, когато насоките са насочени основно към институциите.

Изисквания за уведомяване

Съгласно член 16, параграф 3 от Регламента за ЕБО компетентните органи трябва да уведомят ЕБО дали спазват или възнамеряват да спазват тези насоки, а в противен случай да изложат причините за неспазването им, в срок до 5.5.2015 г. При липса на уведомление до този срок, ЕБО ще счита компетентните органи за неспазващи указанията. Уведомленията следва да се изпращат чрез подаване на формуляра, предоставен в раздел 5, на адрес: compliance@eba.europa.eu при посочване на „EBA/GL/2014/12“. Уведомленията се подават от лица, оправомощени да докладват за наличието на съответствие от името на техните компетентни органи.

Уведомленията ще бъдат публикувани на уебсайта на ЕБО съгласно член 16, параграф 3.

Дял I – Обхват и дефиниции

Обхват

1. Настоящите насоки определят набор от минимални изисквания в областта на сигурността на плащанията в интернет. Насоките допълват правилата на Директива 2007/64/ЕО [1] („Директива за платежните услуги“, ДПУ) относно изискванията по отношение информацията за платежните услуги и задълженията на доставчиците на платежни услуги във връзка с предоставянето на платежни услуги. Освен това член 10, параграф 4 от Директивата изисква от платежните институции да разполагат с надеждни мерки за управление и подходящи механизми за вътрешен контрол.

2. Насоките се прилагат спрямо предоставянето на платежни услуги, предлагани чрез интернет от доставчици на платежни услуги, съгласно определението в член 1 от Директивата.

3. Насоките са предназначени за финансовите институции, както са определени в член 4, параграф 1 от Регламент (ЕС) № 1093/2010, и компетентните органи, определени в член 4, параграф 2 от Регламент (ЕС) № 1093/2010. Компетентните органи в 28-те държави членки на Европейския съюз следва да гарантират прилагането на настоящите насоки от доставчиците на платежни услуги, определени в член 1 от ДПУ, които са под техен надзор.

4. В допълнение, компетентните органи могат да решат да изискат от доставчиците на платежни услуги да докладват пред компетентния орган, че спазват насоките.

5. Насоките не засягат валидността на „Препоръки за сигурността на плащания в интернет“, издадени от Европейската централна банка („Докладът“).[2] С други думи, Докладът продължава да бъде документът, въз основа на който централните банки, при изпълнение на функцията им за надзор над платежните системи и инструменти, оценяват спазването на изискванията за сигурност на плащанията в интернет.

6. Насоките представят минималните очаквания. Те не отменят отговорността на доставчиците на платежни услуги да наблюдават и оценяват рисковете, свързани с извършваните от тях платежни операции, да разработват собствени подробни политики за сигурност и да прилагат подходящи мерки за сигурност, непредвидени ситуации, управление на извънредни ситуации и непрекъснатост на стопанската дейност, които да са съизмерими с рисковете, присъщи на предоставянето на платежни услуги.

[1] Директива 2007/64/ЕО на Европейския парламент и на Съвета от 13 ноември 2007 г. относно платежните услуги във вътрешния пазар, за изменение на директиви 97/7/ЕО, 2002/65/ЕО, 2005/60/ЕО и 2006/48/ЕО и за отмяна на Директива 97/5/ЕО, ОВ L 319, 5.12.2007 г.,

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

7. Целта на насоките е да се определят общи минимални изисквания за изброените по-долу услуги за плащания в интернет, независимо от използваното средство за достъп:

   - [карти] извършване на картови плащания в интернет, включително с виртуални кредитни карти, както и регистриране на данни за картови плащания, които се използват при „портфейлни решения“;

   - [кредитни преводи] изпълнение на кредитни преводи (КП) в интернет;

   - [електронен мандат] издаване и изменение на електронни мандати с директен дебит;

   - [електронни пари] преводи на електронни пари между две сметки с електронни пари чрез интернет.

8. В случаите, когато насоките посочват даден резултат, резултатът може да бъде постигнат чрез различни средства. В допълнение към изложените по-долу изисквания, настоящите насоки предоставят също примери за добри практики (в Приложение 1), които доставчиците на платежни услуги се насърчават, но не се задължават да следват.

9. Ако предоставянето на платежни услуги и инструменти се предлага чрез платежна схема (напр. схеми за картови плащания, схеми за кредитни преводи, схеми за директен дебит и т.н.), компетентните органи и съответната централна банка с надзорна функция върху платежните инструменти следва си сътрудничат, за да осигурят последователно прилагане на насоките от органите, отговорни за функционирането на схемата.

10. Платежните интегратори[3], предлагащи услуги за иницииране на плащания, се считат за приобретатели на платежни услуги в интернет (поради това и като доставчици на платежни услуги) или за външни доставчици на технически услуги на съответните схеми или доставчици на платежни услуги. В последния случай платежните интегратори следва да бъдат задължени по договор да спазват тези насоки.

11. От обхвата на насоките се изключват:

   - други интернет услуги, предоставяни от доставчика на платежни услуги чрез неговия уебсайт за плащания (напр. електронно брокерство, онлайн договори);

   - плащания, при които указанията са дадени по пощата, нареждане по телефона, гласова поща или с помощта на SMS-базирана технология;

   - мобилни плащания, различни от плащания чрез браузър;

[3] Платежните интегратори предоставят на получателя (т.е. електронния търговец) стандартизиран интерфейс за услуги за иницииране на плащания, предоставяни от доставчиците на платежни услуги.

- кредитни преводи (КП), при които трета страна има достъп до платежната сметка на клиента;

- платежни трансакции, извършени от предприятие чрез специални мрежи;

- картови плащания, при които се използват анонимни и непрезареждащи се физически или виртуални предплатени карти, когато няма текущи отношения между картоиздателя и картодържателя;

- клиринг и сетълмент на платежни трансакции.

Дефиниции

12. За целите на настоящите насоки и в допълнение към дефинициите в ДПУ се прилагат следните дефиниции:

- *Удостоверяване на автентичността* означава процедурата, която позволява на доставчика на платежни услуги да провери самоличността на клиента.

- *Задълбочено удостоверяване на автентичността на клиента* за целите на настоящите насоки е процедура, която се основава на използването на два или повече от следните елементи – категоризирани като знания, собственост и принадлежност: i) нещо, което само ползвателят знае, напр. статична парола, код, личен идентификационен код; ii) нещо, което само ползвателят притежава, напр. токен, карта с чип, мобилен телефон; iii) нещо, което е присъщо на ползвателя, напр. биометрични данни като пръстов отпечатък. Освен това избраните елементи трябва да са независими един от друг, т.е. нарушаването на един елемент не влияе на надеждността на друг(и). Най-малко един от елементите следва да бъде еднократен и невъзпроизводим (с изключение на принадлежността) и да не може да бъде откраднат тайно чрез интернет. Процедурата за задълбочено удостоверяване на автентичността на клиента следва да е проектирана по начин, който защитава поверителността на данните за удостоверяване.

- *Оторизация* означава процедура, при която се проверява дали даден клиент или доставчик на платежни услуги има правото да извършва определено действие, напр. правото да прехвърля средства, или да има достъп до чувствителни данни.

- *Удостоверяване на самоличност* е информацията, обикновено поверителна, която се предоставя от клиент или доставчик на платежни услуги с цел удостоверяване на автентичността. „Удостоверяване на самоличност“ може също така да означава физическият инструмент, съдържащ информацията (напр. генератор на еднократни пароли, карта с чип) или нещо, което ползвателят запаметява или го характеризира (напр. биометрични данни).

- *Сериозен инцидент със сигурността* означава инцидент, който има или може да има съществено въздействие върху сигурността, целостта или непрекъснатостта на системите, свързани с плащания на доставчиците на платежни услуги и/или върху сигурността на чувствителни данни за плащанията или средствата. При оценяване на съществеността следва да се вземат предвид броят на потенциално засегнатите ползватели, сумата, изложена на риск, и въздействието върху други доставчици на платежни услуги или други платежни инфраструктури.

- *Анализ на риска при трансакция* означава оценка на рискове, свързани с конкретна трансакция, като се вземат предвид критерии като платежни модели на клиента (поведение), стойност на свързаната трансакция, тип на продукта и профил на получателя.

- *Виртуални карти* означава картово-базиран метод за плащане, при който се генерира алтернативен, временен номер на карта с намален срок на валидност, ограничена употреба и с предварително определен лимит на харчене, който може да се използва за интернет покупки.

- *Портфейлни решения* означава решения, при които ползвателят може да регистрира данни за един или повече платежни инструменти с цел извършване на плащания към няколко електронни търговци.

Дял II - Насоки относно сигурността на плащанията в интернет

Обща среда за контрол и сигурност

Управление

1. Доставчиците на платежни услуги следва да прилагат официална политика за сигурност за услугите за плащане в интернет и редовно да я преразглеждат.

   1.1 Политиката за сигурност следва да бъде надлежно документирана и да се преразглежда редовно (в съответствие с насока 2.4), както и да бъде одобрена от висшето ръководство. Тя следва да определя целите в областта на сигурността и склонността към поемане на рискове.

   1.2 Политиката за сигурност следва да определя ролите и отговорностите, включително функцията за управление на риска при пряка йерархична подчиненост към управителния съвет и йерархична подчиненост за предоставяните услуги за плащане в интернет, включително управление на чувствителни данни за плащанията по отношение на оценката, контрола и намаляването на риска.

Оценка на риска

2. Доставчиците на платежни услуги следва да извършват и документират цялостни оценки на риска по отношение на сигурността на плащанията в интернет и свързаните с тях услуги, преди да създадат услугата(ите) и периодично след това.

   2.1 Чрез своята функция за управление на риска доставчиците на платежни услуги следва да извършват и документират подробни оценки на риска за плащанията в интернет и свързаните с тях услуги. Доставчиците на платежни услуги следва да вземат предвид резултатите от текущото наблюдение на заплахите за сигурността във връзка с услугите за плащане в интернет, които предлагат или планират да предлагат, като отчитат: i) използваните от тях технологични решения, ii) услугите, възложени на външни доставчици, и iii) техническата среда на клиентите. Доставчиците на платежни услуги следва да вземат предвид рисковете, свързани с избраните технологични платформи, архитектура на приложенията, техниките за програмиране и рутината от тяхна страна[4] и от страна на клиентите[5], както и резултатите от процеса на наблюдение за инциденти, свързани със сигурността (вж. насока 3).

[4] Напр. податливостта на системата към отвличане на платежна сесия, внедряване на SQL код, междусайтово скриптиране, претоварване на буферите и др.

[5] Напр. рискове, свързани с използването на мултимедийни приложения, добавки към браузъра, рамки, външни връзки и др.

2.2 На тази основа доставчиците на платежни услуги следва да определят дали и до каква степен може да са необходими промени на съществуващите мерки за сигурност, използваните технологии и предлаганите процедури или услуги. Доставчиците на платежни услуги следва да вземат под внимание времето, необходимо за въвеждане на промените (вкл. добавяне на нови клиенти), и да предприемат подходящите междинни мерки, за да сведат до минимум инцидентите и измамите в областта на сигурността, както и потенциалните неблагоприятни последици.

2.3 В оценката на рисковете следва да се обърне внимание на необходимостта от опазване и защита на чувствителни данни за плащанията.

2.4 Доставчиците на платежни услуги следва да направят преглед на рисковите сценарии и съществуващите мерки за сигурност след сериозни инциденти, засягащи техните услуги, преди извършването на значителна промяна в инфраструктурата или процедурите и при идентифицирането на нови заплахи чрез наблюдение на рисковете. В допълнение, най-малко веднъж годишно следва да се извършва общ преглед на оценката на риска. Резултатите от оценката на риска и прегледите следва да бъдат представени пред висшето ръководство за одобрение.

Наблюдение и докладване на инциденти

3. Доставчиците на платежни услуги следва да осигурят последователно и интегрирано наблюдение, обработка и проследяване на инцидентите със сигурността, включително оплаквания на клиенти относно сигурността. Доставчиците на платежни услуги следва да установят процедура за докладване на такива инциденти пред ръководството, а в случай на сериозни инциденти със сигурността на плащанията — пред компетентните органи.

3.1 Доставчиците на платежни услуги следва да прилагат процедура за наблюдение, обработка и проследяване на инциденти със сигурността и оплаквания на клиенти относно сигурността, и да докладват такива инциденти пред ръководството.

3.2 Доставчиците на платежни услуги следва да разполагат с процедура за незабавно уведомяване на компетентните органи (т.е. надзорните органи и органите за защита на личните данни), ако съществуват такива, в случай на сериозни инциденти със сигурността на плащанията, свързани с предоставените от тях платежни услуги.

3.3 Доставчиците на платежни услуги следва да имат процедура за сътрудничество със съответните правоприлагащи служби при сериозни инциденти със сигурността на плащанията, включително нарушения на сигурността на личните данни.

3.4 Акцептиращите доставчици на платежни услуги следва чрез договор да изискват от електронните търговци, които съхраняват, обработват или предават чувствителни данни за плащанията, да си сътрудничат при сериозни инциденти със сигурността на плащанията, включително нарушения на сигурността на личните данни, както с тях, така и със съответните правоприлагащи служби. Ако доставчик на платежни услуги узнае, че електронен търговец не сътрудничи, както се изисква по силата на договор, той следва да вземе мерки, за да приложи това договорно задължение, или да прекрати договора.

Контрол и намаляване на риска

4. Доставчиците на платежни услуги следва да прилагат мерки за сигурност в съответствие със своите политики за сигурност, за да се намалят идентифицираните рискове. Тези мерки следва да включват няколко нива на защита на сигурността, при което провалът на една защитна линия се прихваща от следващата защитна линия („защита в дълбочина“).

4.1 При проектиране, разработване и поддържане на услуги за плащания в интернет, доставчиците на платежни услуги следва да обърнат специално внимание на подходящото разпределение на задълженията в средите на информационните технологии (ИТ) (напр. развойна, тестова и производствена среда) и на правилното прилагане на принципа на „най-малката привилегия“ като основа за добро управление на идентичността и достъпа. [6]

4.2 Доставчиците на платежни услуги следва да прилагат подходящи решения за сигурност, за да защитят мрежите, уебсайтовете, сървърите и комуникационните връзки срещу злоупотреба или атаки. Доставчиците на платежни услуги следва да премахнат от сървърите всички излишни функции, за да ги защитят (засилят) и да отстранят или намалят уязвимостта на приложенията, изложени на риск. Достъпът чрез различни приложения до търсените данни и източници трябва да бъде сведен до строг минимум при спазване на принципа за „най-малка привилегия“. За да се ограничи използването на „фалшиви“ уебсайтове (имитиращи законните сайтове на доставчиците на платежни услуги), уебсайтовете за трансакции, които предлагат услуги за плащания в интернет, трябва да се идентифицират чрез разширени сертификати за валидиране, съставени на името на доставчика на платежни услуги, или чрез други подобни методи за удостоверяване на автентичността.

4.3 Доставчиците на платежни услуги следва да прилагат подходящи процедури за наблюдение, проследяване и ограничаване достъпа до: i) чувствителни данни за плащанията и ii) важни логически и физически ресурси, например мрежи,

[6] „Всяка програма и всеки привилегирован ползвател на системата трябва да работи, като използва най-малкото количество привилегия, необходима за изпълнение на задачата“. Вж. Saltzer, J. H. (1974), ‘Protection and the Control of Information Sharing in Multics’, Communications of the ACM, Vol. 17, No 7, p. 388.

системи, бази данни, защитни модули и др. Доставчиците на платежни услуги следва да създадат, съхраняват и анализират подходящи регистри и одитни пътеки.

4.4 При проектиране[7], разработване и поддържане на услуги за плащания в интернет, доставчиците на платежни услуги следва да гарантират, че свеждането на данните до минимум[8] е съществен елемент от основните функционални възможности: събирането, маршрутизирането, обработването, съхраняването и/или архивирането, както и визуализацията на чувствителни данни за плащанията трябва да се поддържат на абсолютно минимално ниво.

4.5 Мерките за сигурност по отношение на услугите за плащания в интернет следва да бъдат тествани под контрола на функцията за управление на риска, за да се гарантира тяхната устойчивост и ефективност. Всички промени следва да са предмет на формален процес на управление на промените, който гарантира, че промените са надлежно планирани, тествани, документирани и оторизирани. Предвид направените промени и установените заплахи за сигурността, тестовете трябва да се повтарят периодично и да включват сценарии на свързани и известни потенциални атаки.

4.6 Използваните от доставчиците на платежни услуги мерки за сигурност по отношение на услугите за плащания в интернет следва да бъдат периодично одитирани, за да се гарантира тяхната устойчивост и ефективност. Прилагането и функционирането на услугите за плащания в интернет също трябва да бъдат одитирани. Честотата и акцентът на такива одити зависят и са пропорционални на свързаните рискове за сигурността. Одитите следва да се извършват от надеждни и независими (вътрешни или външни) експерти. Те по никакъв начин не трябва да участват в разработването, изпълнението или оперативното управление на предоставяните услуги за плащания в интернет.

4.7 В случай че доставчиците на платежни услуги възлагат на външни изпълнители функции, свързани със сигурността на услугите за плащания в интернет, договорът трябва да включва клаузи, които изискват спазването на принципите и насоките, изложени в настоящите насоки.

4.8 Доставчиците на платежни услуги, които предлагат услуги по акцептиране, следва чрез договор да изискват от електронните търговци, които работят (т.е. съхраняват, обработват или предават) с чувствителни данни за плащанията, да въведат мерки за сигурност в тяхната ИТ инфраструктура, в съответствие с насоки 4.1 до 4.7, за да се избегне кражба на чувствителни данни за плащанията през

[7] Поверителност при проектиране.

[8] Свеждането на данните до минимум се отнася до политиката за събиране на най-малкото количество лична информация, която е необходима за извършването на дадена функция.

техните системи. Ако доставчик на платежни услуги узнае, че електронен търговец не разполага с необходимите мерки за сигурност, той трябва да вземе мерки, за да приложи това договорно задължение, или да прекрати договора.

Проследимост

5. Доставчиците на платежни услуги следва да прилагат процедури, които гарантират, че всички трансакции, както и процесът на протичане на електронния мандат, се проследяват подходящо.

5.1 Доставчиците на платежни услуги следва да гарантират, че тяхната услуга включва механизми за сигурност за подробно регистриране на трансакцията, както и данни за електронния мандат, включително пореден номер на трансакцията, клеймо с дата и час за данните на трансакцията, промени в параметрирането и достъп до данни за трансакцията и електронния мандат.

5.2 Доставчиците на платежни услуги следва да въведат регистрационни файлове, които позволяват да се проследи всяко добавяне, промяна или заличаване на данни за трансакцията и електронния мандат.

5.3 Доставчиците на платежни услуги следва да подлагат на проверка и да анализират данните за трансакцията и електронния мандат и да гарантират, че разполагат с инструменти за оценка на регистрационните файлове. Съответните приложения следва да се предоставят на разположение само на оторизиран персонал.

Специфични мерки за контрол и сигурност на плащанията в интернет

Първоначална идентификация на клиент, информация

6. Клиентите следва да бъдат надлежно идентифицирани в съответствие с европейското законодателство срещу прането на пари[9] и да потвърдят своето желание да извършат плащания в интернет с помощта на услугите, преди да им бъде предоставен достъп до такива услуги. Доставчиците на платежни услуги следва да предоставят подходяща „предварителна“, „редовна“ или, ако е приложимо, „извънредна“ информация на клиента за необходимите изисквания (напр. оборудване, процедури) за извършване на сигурни платежни трансакции в интернет и за свързаните с това рискове.

[9] Напр. Директива 2005/60/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 г. за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризъм. ОВ L 309, 25.11.2005 г., стр. 15-36. Вж. също Директива 2006/70/ЕО на Комисията от 1 август 2006 г. относно установяването на мерки за прилагане на Директива 2005/60/ЕО на Европейския парламент и на Съвета по отношение на определението „видни политически личности“ и техническите критерии за процедурите по опростена проверка на клиентите и за изключения поради финансова дейност на случайна или много ограничена база. ОВ L 214, 4.8.2006 г., стр. 29-34.

6.1 Доставчиците на платежни услуги следва да гарантират, че клиентът е преминал процедурите по проверка на клиентите и е предоставил подходящи документи за самоличност[10] и свързана информация, преди да му бъде предоставен достъп до услуги за плащания в интернет[11].

6.2 Доставчиците на платежни услуги следва да гарантират, че предварителната информация[12], предоставена на клиента, съдържа конкретни данни относно услугите за плащания в интернет. Те следва да включват, ако е подходящо:

- ясна информация за всички изисквания по отношение на клиентското оборудване, софтуер или други необходими инструменти (напр. антивирусен софтуер, защитни стени);
- насоки за правилната и сигурна употреба на персонализирани сертификати за сигурност;
- поетапно описание на процедурата за подаване и оторизиране на платежна трансакция от страна на клиента и/или за получаване на информация, включително последствията от всяко действие;
- насоки за правилната и сигурна употреба на хардуер и софтуер, предоставени на клиента;
- процедурите, които трябва да се следват в случай на загуба или кражба на персонализирана защитна удостоверителна информация, хардуера или софтуера на клиента за влизане или извършване на трансакции;
- процедурите, които трябва да се следват при установена или предполагаема злоупотреба;
- описание на отговорностите и задълженията, съответно, на доставчиците на платежни услуги и на клиента по отношение на използването на услугата за плащане в интернет.

6.3 Доставчиците на платежни услуги следва да гарантират, че в рамковия договор с клиента е посочено, че доставчикът на платежни услуги може да блокира

[10] Напр. паспорт, национална лична карта или усъвършенстван електронен подпис.

[11] Процесът на идентификация на клиента не засяга изключения, предвидени в съществуващото законодателство срещу прането на пари. Доставчиците на платежни услуги не е необходимо да провеждат отделен процес за идентификация на клиента за услуги за плащане в интернет, при условие че такава идентификация вече е извършена, напр. за други съществуващи услуги, свързани с плащане, или за откриването на сметка.

[12] Тази информация допълва член 42 от ДПУ, който посочва информацията, която доставчикът на платежни услуги трябва да предостави на ползвателя на платежни услуги преди сключването на договор за предоставяне на платежни услуги.

конкретна трансакция или платежния инструмент[13] от съображения за сигурност. Договорът следва да определя метода и условията за известяване на клиента и начина, по който клиентът може да се свърже с доставчика на платежни услуги за „отблокиране“ на трансакцията или услугата за плащане в интернет, в съответствие с ДПУ.

Задълбочено удостоверяване на автентичността на клиента

7. Иницииране на плащания в интернет, както и достъпът до чувствителни данни за плащанията, следва да бъдат защитени чрез задълбочено удостоверяване на автентичността на клиента. Доставчиците на платежни услуги трябва да разполагат с процедура за задълбочено удостоверяване на автентичността на клиента в съответствие с определението в настоящите насоки.

7.1 [КП/електронен мандат/електронни пари] (Доставчиците на платежни услуги следва да извършват задълбочено удостоверяване на автентичността на клиента с цел оторизиране на плащания в интернет от страна на клиента (включително пакетни КП) и с цел издаването или изменението на електронни мандати за директен дебит. Доставчиците на платежни услуги могат обаче да обмислят възможността да приемат алтернативни мерки за удостоверяване на автентичността на клиента с цел:

- изходящи плащания към надеждни бенефициенти, включени в предварително установени бели списъци за този клиент;
- трансакции между две сметки на един клиент при един и същ доставчик на платежни услуги;
- преводи в рамките на един и същ доставчик на платежни услуги, обосновани чрез анализ на риска от трансакцията;
- малки плащания, както е посочено в ДПУ [14].

7.2 Получаването на достъп до или изменението на чувствителни данни за плащанията (вкл. създаване и изменение на бели списъци) изисква задълбочено удостоверяване на автентичността на клиента. Ако доставчикът на платежни услуги предлага чисто консултантски услуги без показване на чувствителна клиентска или платежна информация, напр. данни за разплащателната карта, с която лесно би могло да се злоупотреби с цел извършване на измама,

[13] Вж. член 55 от ДПУ за ограниченията за използване на платежния инструмент.

[14] Вж. определението на инструменти за малки плащания в член 34, параграф 1 и член 53, параграф 1 от ДПУ.

доставчикът на платежни услуги може да адаптира изискванията си за удостоверяване на автентичността въз основа на оценката на риска.

7.3 [карти] При операции с карти всички доставчици на платежни услуги, които издават карти, следва да поддържат задълбочено удостоверяване на автентичността на картодържателя. Всички издадени карти следва да бъдат технически готови (регистрирани) за използване със задълбочено удостоверяване на автентичността.

7.4 [карти] Доставчиците на платежни услуги, които предлагат услуги по акцептиране, следва да поддържат технологии, позволяващи на картоиздателя да извършва задълбочено удостоверяване на автентичността на картодържателя при схеми за картови плащания, в които участва акцептиращият доставчик на платежни услуги.

7.5 [карти] Доставчиците на платежни услуги, които предлагат услуги по акцептиране, следва да изискват от своите електронни търговци да поддържат решения, позволяващи на картоиздателя да извършва задълбочено удостоверяване на автентичността на картодържателя при извършването на операции с карти през интернет. Използването на мерки за алтернативно удостоверяване на автентичността може да се обмисли по отношение на предварително определени категории нискорискови трансакции, напр. въз основа на анализа на риска от трансакцията, или които включват малки плащания, както е посочено в ДПУ.

7.6 [карти] По отношение на приетите от услугата схеми за картови плащания доставчиците на портфейлни решения следва да изискват задълбочено удостоверяване на автентичността от картоиздателя, ако законният картодържател регистрира данните на картата за първи път.

7.7 Доставчиците на портфейлни решения следва да поддържат задълбочено удостоверяване на автентичността на клиента в случаите, когато клиентите влизат в портфейлните платежни услуги или извършват операции с карти през интернет. Използването на мерки за алтернативно удостоверяване на автентичността може да се обмисли по отношение на предварително определени категории нискорискови трансакции, напр. въз основа на анализа на риска от трансакцията, или които включват малки плащания, както е посочено в ДПУ.

7.8 [карти] По отношение на виртуалните карти първоначалната регистрация следва да се проведе в безопасна и надеждна среда [15]. Ако картата е издадена в

[15] Средите, за които доставчиците на платежни услуги носят отговорност и при които се гарантира подходящо удостоверяване на автентичността на клиента и на доставчика на платежни услуги, предлагащ услугата, и защита на поверителна/чувствителна информация, включват: i) помещенията на доставчика на платежни услуги; ii) уебсайт за интернет банкиране или друг защитен уебсайт, напр. в който GA предлага сравними защитни характеристики *inter alia*, както е определено в насока 4; или iii) банкоматни (ATM) услуги. (в случая с ATM се изисква задълбочено удостоверяване на автентичността на клиента. Такова удостоверяване на автентичността обикновено се извършва чрез чип и PIN или чрез чип и биометрични данни).

интернет среда, за процеса на генериране на данни за виртуалната карта следва да се изисква задълбочено удостоверяване на автентичността на клиента.

7.9 Доставчиците на платежни услуги следва да гарантират подходящо двустранно удостоверяване на автентичността, когато комуникират с електронните търговци с цел иницииране на плащания в интернет и достъп до чувствителни данни за плащанията.

Записване за и предоставяне на инструменти за удостоверяване на автентичността и/или софтуер, доставен на клиента

8. Доставчиците на платежни услуги следва да гарантират, че записването на клиента и първоначалното предоставяне на инструменти за удостоверяване на автентичност, необходими за използване на услугата за плащания в интернет и/или доставяне на клиентите на софтуер, свързан с плащания, се извършва по сигурен начин.

8.1 Записването и предоставянето на инструменти за удостоверяване на автентичността и/или софтуер, свързан с плащания, доставен на клиента, трябва да отговарят на следните изисквания:

- Съответните процедури трябва да се извършват в безопасна и надеждна среда, като се вземат предвид възможните рискове, произтичащи от устройствата, които не са под контрола на доставчика на платежни услуги.

- Трябва да се прилагат ефективни и сигурни процедури за доставка на персонализирани сертификати за сигурност, софтуер за извършване на плащания и всички персонализирани устройства, свързани с плащанията в интернет. Софтуерът, който се доставя през интернет, трябва също да се подпише електронно от доставчика на платежни услуги, за да позволи на клиента да провери неговата автентичност и че не е бил подправен.

- [карти] По отношение на операциите с карти клиентът трябва да има възможност да се регистрира за задълбочено удостоверяване на автентичността независимо от конкретна покупка по интернет. Ако по време на онлайн пазаруване се предлага активация, това трябва да се извърши чрез пренасочване на клиента към безопасна и надеждна среда.

8.2 [карти] Картоиздателите следва активно да насърчават картодържателите да се записват за задълбочено удостоверяване на автентичността и да разрешават избягване на записването само при изключителни и ограничен брой случаи, ако това е оправдано от риска, свързан с конкретната операция с карта.

Опити за влизане, изтичане на сесията, валидност на удостоверяването на автентичността

9. Доставчиците на платежни услуги следва да ограничат броя на опитите за влизане или удостоверяване на автентичността, да определят правила за „изтичане“ на сесията при услуги за плащания в интернет и да установят времеви лимити за валидността на удостоверяването на автентичността.

   9.1 При използване на еднократна парола (one-time password „OTP“) с цел удостоверяване на автентичността, доставчиците на платежни услуги следва да гарантират, че периодът на валидност на такива пароли е строго ограничен до необходимия минимум.

   9.2 Доставчиците на платежни услуги следва да определят максималния брой неуспешни опити за влизане или удостоверяване на автентичността, след който (временно или за постоянно) се блокира достъпът до услугата за плащане в интернет. Те трябва да прилагат сигурна процедура за реактивация на блокираните услуги за плащане в интернет.

   9.3 Доставчиците на платежни услуги трябва да определят максималния период, след който неактивните услуги за плащане в интернет се прекратяват автоматично.

Наблюдение на трансакциите

10. Механизмите за наблюдение на трансакции, предназначени да предотвратяват, засичат и блокират измамни платежни трансакции, следва да се активират преди окончателното оторизиране от страна на доставчика на платежни услуги; подозрителните или високорискови трансакции следва да подлежат на специфична процедура за скрининг и оценка. Равностойни механизми за наблюдение на сигурността и удостоверяване на автентичността следва да се прилагат и за издаване на електронни мандати.

    10.1 Доставчиците на платежни услуги следва да използват системи за засичане и предотвратяване на измами, за да идентифицират подозрителните трансакции, преди доставчикът на платежни услуги окончателно да оторизира трансакции или електронни мандати. Тези системи следва да се основават, например, на параметризирани правила (напр. черни списъци на компрометирани или откраднати данни за картата) и да проследяват необичайни модели на поведение на клиента или на клиентското устройство за достъп (напр. промяна в IP (интернет протокол) адреса[16] или IP обхват по време на сесия на услуги за плащане в интернет, понякога идентифицирани чрез географско позициониране на IP

[16] IP адресът е уникален числов код, идентифициращ всеки компютър, свързан към интернет.

адреса[17], нетипични категории електронни търговци за конкретен клиент или необичайни трансакционни данни и др.). Системите следва също да бъдат в състояние да откриват признаци на злонамерена софтуерна инфекция по време на сесията (напр. чрез *script versus human validation*) и известни измамни сценарии. Степента, сложността и капацитетът за адаптиране на решенията за проследяване, при спазване на съответното законодателство за защита на данните, следва да бъдат съобразени с резултата от оценката на риска.

10.2 Акцептиращите доставчици на платежни услуги следва да прилагат системи за откриване и предотвратяване на измами, за да проследяват дейностите на електронните търговци.

10.3 Доставчиците на платежни услуги следва да изпълняват всяка процедура по скрининг и оценка на трансакция в рамките на подходящ период от време, с цел да не се забавя излишно инициирането и/или изпълнението на съответната платежна услуга.

10.4 В случай че, съгласно своята политика за риска, доставчикът на платежни услуги реши да блокира платежна трансакция, която е била определена като потенциално измамна, доставчикът на платежни услуги следва да поддържа блокирането за възможно най-кратък период до разрешаване на проблемите със сигурността.

Защита на чувствителни данни за плащанията

11. Чувствителните данни за плащанията следва да бъдат защитени, когато се съхраняват, обработват или предават.

11.1 Всички данни, използвани за идентифициране и удостоверяване на автентичността на клиенти (напр. при влизане, при иницииране на плащания в интернет и при издаване, изменение или отмяна на електронни мандати), както и клиентският интерфейс (уебсайт на доставчик на платежни услуги или електронен търговец), следва да бъдат подходящо защитени срещу кражба и неоторизиран достъп или модификация.

11.2 Доставчиците на платежни услуги следва да гарантират, че когато обменят чувствителни данни за плащанията през интернет, между комуникиращите страни се прилага защитено *end-to-end* криптиране [18] през цялата комуникационна сесия, за да защитят поверителността и целостта на данните, като използват силни и широко признати техники за криптиране.

[17] „Гео-IP“ проверката проверява дали издаващата държава съответства на IP адреса, от който ползвателят инициира трансакцията.

[18] *End-to-end* криптиране означава криптиране в рамките на и при системата на крайния източник, като съответното декриптиране настъпва само в рамките на или при системата на крайната дестинация. ETSI EN 302 109 V1.1.1. (2003-06).

11.3 Доставчиците на платежни услуги, които предлагат услуги по акцептиране, следва да насърчават своите електронни търговци да не съхраняват чувствителни данни за плащанията. В случай че електронни търговци работят, т.е. съхраняват, обработват или предават чувствителни данни за плащанията, такива доставчици на платежни услуги следва чрез договор да изискват от електронните търговци да прилагат необходимите мерки за защита на тези данни. Доставчиците на платежни услуги следва да извършват редовни проверки и ако доставчик на платежни услуги узнае, че електронен търговец, който работи с чувствителни данни за плащанията, не разполага с необходимите мерки за сигурност, той трябва да вземе мерки, за да приложи това договорно задължение, или да прекрати договора.

Информираност, обучение и комуникация с клиента

Обучение и комуникация с клиента

12. Доставчиците на платежни услуги следва да предоставят помощ и указания на клиентите, ако е необходимо, по отношение на сигурната употреба на услуги за плащания в интернет. Доставчиците на платежни услуги следва да комуникират с клиентите си по такъв начин, че да ги убедят в автентичността на получените съобщения.

12.1 Доставчиците на платежни услуги следва да осигурят най-малко един защитен канал[19] за текуща комуникация с клиенти по отношение на правилната и сигурна употреба на услуги за плащания в интернет. Доставчиците на платежни услуги следва да информират клиентите за този канал и да обяснят, че всяко съобщение от името на доставчика на платежни услуги, изпратено чрез други средства, например електронна поща, което се отнася до правилната и сигурна употреба на услугата за плащане в интернет, не е надеждно. Доставчикът на платежни услуги следва да обясни:

- процедурата за докладване от страна на клиентите пред доставчика на платежни услуги на (предполагаеми) подправени плащания, подозрителни инциденти или аномалии по време на сесии на услуги за плащания в интернет и/или възможни опити за социален инженеринг[20];

- следващите стъпки, т.е. как доставчикът на платежни услуги ще отговори на клиента;

[19] Напр. специална пощенска кутия на уебсайта на доставчика на платежни услуги или защитена страница.

[20] Социалният инженеринг в този контекст означава техники за манипулиране на хората с цел получаване на информация (напр. чрез имейл или телефонни обаждания) или изтегляне на информация от социални мрежи с цел измама или получаване на неоторизиран достъп до компютър или мрежа.

- как доставчикът на платежни услуги ще уведоми клиента за (потенциални) подправени трансакции или тяхното неинициране, или ще предупреди клиента за появата на атаки (напр. phishing e-mails).

12.2 Чрез защитения канал доставчиците на платежни услуги следва да информират клиентите за актуализации в процедурите за сигурност относно услугите за плащания в интернет. Всички предупреждения за значителни възникващи рискове (напр. предупреждения за социален инженеринг) следва също да се предоставят през защитения канал.

12.3 Доставчиците на платежни услуги следва да предоставят на клиента достъп до помощ по всички въпроси, жалби, молби за поддръжка и известия за аномалии или инциденти по отношение на плащанията в интернет и свързаните с тях услуги, като клиентите следва да бъдат информирани по подходящ начин как може да получат тази помощ.

12.4 Доставчиците на платежни услуги следва да инициират програми за обучение и осведомяване на клиента, предназначени да гарантират, че клиентите разбират най-малкото необходимостта от:

- защита на паролите, защитните знаци, личните данни и друга поверителна информация;

- правилно управление на сигурността на личното устройство (напр. компютър) чрез инсталиране и актуализиране на защитни компоненти (антивирусни програми, защитни стени, защитни пачове);

- отчитане на значителните заплахи и рискове, свързани със сваляне на софтуер през интернет, ако клиентът не може да е абсолютно сигурен, че софтуерът е оригинален и не е бил подправен;

- използване на оригиналния уебсайт за плащания в интернет на доставчика на платежни услуги.

12.5 Акцептиращите доставчици на платежни услуги следва да изискват от електронните търговци ясно да отделят процесите, свързани с плащания от онлайн магазина, за да улеснят клиентите при идентифицирането кога да комуникират с доставчиците на платежни услуги, а не с получателя (напр. чрез пренасочване на клиента и отваряне на отделен прозорец, така че платежният процес не се показва в рамката на електронния търговец).

Известия, поставяне на лимити

13. Доставчиците на платежни услуги следва да определят лимити за услуги за плащания в интернет и могат да предоставят на своите клиенти възможности за допълнително

ограничаване на риска в рамките на тези лимити. Те могат също да предоставят услуги за предупреждение и управление на клиентския профил.

13.1 Преди да предоставят на клиента услуги за плащания в интернет, доставчиците на платежни услуги трябва да поставят лимити[21], приложими за тези услуги (напр. максимална сума за всяко отделно плащане или кумулативна сума за определен период от време), като съответно информират своите клиенти. Доставчиците на платежни услуги трябва да позволят на клиентите да дезактивират функционалността на плащания в интернет.

Достъп на клиентите до информация за статуса на иницииране и изпълнение на плащането

14. Доставчиците на платежни услуги следва да потвърдят на клиентите инициирането на плащането и своевременно да предоставят на клиентите необходимата информация, за да проверят дали платежната трансакция е правилно инициирана и/или изпълнена.

14.1 [КП/електронен мандат] (Доставчиците на платежни услуги следва да предоставят на клиентите си средства за проверка почти в реално време на статуса на изпълнението на трансакциите, както и салдата по сметките по всяко време[22] в безопасна и надеждна среда.

14.2 Всички подробни електронни извлечения следва да бъдат предоставени на разположение в безопасна и надеждна среда. Когато доставчиците на платежни услуги информират клиентите за наличието на електронни извлечения (напр. редовно при издаването на периодично електронно извлечение или извънредно след извършването на трансакция) чрез алтернативен канал, като SMS, имейл или писмо, чувствителните данни за плащанията не трябва да бъдат включени в такива съобщения или, ако са включени, трябва да са маскирани.

Дял III - Заключителни разпоредби и прилагане

15. Тези насоки се прилагат от 01.08.2015.

[21] Подобни лимити могат да се прилагат глобално (т.е. за всички платежни инструменти, даващи възможност за плащане в интернет) или индивидуално.

[22] С изключение на извънредното неналичие на средството поради техническа поддръжка или в резултат от сериозни инциденти.

Приложение 1: Примери за добри практики

В допълнение към изискванията, посочени по-горе, настоящите насоки описват някои добри практики, които доставчиците на платежни услуги и съответните участници на пазара се насърчават, но не се задължават да приемат. За удобство разделите, за които се прилагат тези добри практики, са посочени изрично.

Обща среда за контрол и сигурност

Управление

ДП 1: Политиката за сигурност може да бъде изложена в специален документ.

Контрол и намаляване на риска

ДП 2: Доставчиците на платежни услуги могат да осигурят защитни инструменти (напр. правилно защитени устройства и/или персонализирани браузъри) за защита на клиентския интерфейс срещу неправомерно използване или атаки (напр. атаки *„man in the browser“*).

Проследимост

ДП 3: Доставчиците на платежни услуги, които предлагат услуги по акцептиране, могат да изискват от електронните търговци, които съхраняват информация за плащанията, да прилагат подходящи процедури за поддържане на проследимостта.

Специфични мерки за контрол и сигурност на плащанията в интернет

Първоначална идентификация на клиент, информация

ДП 4: Клиентът може да подпише специален договор за услуги за извършване на платежни трансакции в интернет, вместо условията да бъдат включени в по-широк договор за общи услуги с доставчика на платежни услуги.

ДП 5: Доставчиците на платежни услуги могат също да гарантират, че на клиентите се предоставят на текуща база или, ако е приложимо, извънредно, и чрез подходящи средства (напр. листовки, уебсайт страници) ясни и недвусмислени инструкции, които обясняват отговорностите им по отношение на сигурното използване на услугата.

Задълбочено удостоверяване на автентичността на клиента

ДП 6: [карти] (Електронните търговци могат да поддържат задълбочено удостоверяване на автентичността на картодържателя от страна на картоиздателя при извършването на операции с карти през интернет.

ДП 7: За удобство на клиента доставчиците на платежни услуги могат да обмислят възможността за използване на задълбочено удостоверяване на автентичността на

клиента за всички услуги за плащания в интернет. Това може да направи решението по-приемливо за клиентите и да улесни правилното използване.

ДП 8: Задълбоченото удостоверяване на автентичността на клиента може да включва елементи, които свързват удостоверяването на автентичността с конкретна сума и получател. Това може да даде на клиентите повече сигурност при оторизиране на плащания. Технологичното решение, което дава възможност за свързване на данните за задълбочено удостоверяване на автентичността и данните за трансакцията, трябва да е защитено срещу подправяне.

Защита на чувствителни данни за плащанията

ДП 9: Желателно е електронните търговци, които работят с чувствителни данни за плащания, да провеждат подходящо обучение на персонала за управление на измами и да актуализират това обучение редовно, за да де гарантира, че съдържанието не губи връзка с динамичната среда на сигурността.

Обучение и комуникация с клиента

ДП 10: Желателно е доставчиците на платежни услуги, които предлагат услуги по акцептиране, да организират за своите електронни търговци програми за обучение по предотвратяване на измами.

Известия, поставяне на лимити

ДП 11: В рамките на зададените лимити доставчиците на платежни услуги могат да предоставят на своите клиенти възможността да управляват лимитите на услугите за плащания в интернет в безопасна и надеждна среда.

ДП 12: Доставчиците на платежни услуги могат да въведат предупреждения за клиентите, например чрез телефонни обаждания или чрез SMS, за подозрителни или високорискови платежни трансакции въз основа на своите политики за управление на риска.

ДП 13: Доставчиците на платежни услуги могат да дадат възможност на клиентите да определят общи, персонализирани правила като параметри за тяхното поведение във връзка с плащанията в интернет и свързаните с тях услуги, например, че те могат да инициират плащания само от конкретни държави и че плащания, инициирани от друго място, следва да бъдат блокирани, както и че те могат да включат конкретни получатели в бели или черни списъци.