DATA AND SECURITY INCIDENT REPORTING UNDER GDPR, PSD2, NISD AND EIDAS REGULATION

The recent regulatory focus on cyber-security and data protection can be seen in a number of new requirements on firms to notify regulators – and in some cases affected individuals – of data and security breaches and other operational incidents. This briefing looks across these requirements and highlights areas of overlap as well as differences between the regimes.

Key issues

- GDPR, PSD2, NISD and eIDAS Regulation introduce incident reporting regimes
- There is some overlap between these regimes, to notify regulators of data breaches, security or operational incidents
- Each regime has its own tests for when the notification requirement is triggered, who should be notified and information to be provided
- In some cases, firms must also notify affected users or individuals, or even the public
- Timeframes for notifications can be short, especially under PSD2 where the initial report must be submitted within four hours
- Detailed requirements are set out in guidelines for each regime

OVERVIEW

During the first half of 2018, some firms will become subject to three new incident reporting regimes under the General Data Protection Regulation (GDPR), the recast Payment Services Directive (PSD2) and the Network and Information Security Directive (NISD).

A similar incident reporting regime under the eIDAS Regulation, applicable to trust service providers (broadly firms that create, verify, validate or preserve electronic signatures, electronic seals, electronic timestamps, electronic registered delivery services, related certificates or website certificates) has been in force since July 2016.

There are common themes running through these regimes, which reflect the current regulatory focus on data protection, cyber-security and operational resilience, but the devil will be in the detail as in-scope firms seek to ensure that they have implemented relevant requirements for each regime. In particular, each regime has different triggers for reporting: reports may need to be submitted to various regulators within different timescales and using different reporting templates.

This briefing provides a very short overview of these incident reporting regimes, before highlighting some of the key similarities and differences between them.

GDPR personal data breach reporting

Under the GDPR, data controllers (organisations deciding on the purpose and means of the personal data processing) must (i) notify a personal data breach to the supervisory authority within 72 hours after becoming "aware" of it, and (ii) communicate the personal data breach to the data subject without undue delay.

Data processors (i.e., third party service providers that process personal data on behalf of the controller's customer) must notify controllers without undue delay after becoming "aware" of a personal data breach. Legal responsibility to notify the supervisory authority continues to rest with controllers.

Personal data breach is basically a security incident affecting personal data. The revised guidelines on Personal data breach notification set useful actions and examples to comply with the GDPR.

The GDPR has extraterritorial effect. Operators with no base in the European Union that target offers of goods or services to, or monitor the behaviour of, individuals in the EU, must designate a representative in the European Union and notify personal data breaches to the supervisory authority of the EU Member State where the representative is established.

Major incident reporting under PSD2

Under PSD2, payment service providers (PSPs) are required to notify their home competent authority within 4 hours of becoming aware of a "*major operational or security incident*", as well as providing intermediate status update reports and a final report once root cause analysis has been carried out. Where the incident may have an impact on the financial interests of payment service users (PSUs), the PSP must also inform PSUs of the incident and mitigation measures without undue delay.

When drafting its guidelines on these requirements, the EBA acknowledged the existence of other incident reporting frameworks but explained that it was not able to harmonise criteria, templates and notification processes across different regimes as its mandate was limited to PSD2. However, the EBA did note that it has tried to align the PSD2 guidelines with the Single Supervisory Mechanism (SSM) cyber-incident reporting framework, which the ECB implemented as a pilot scheme in 2016 and rolled out to other significant institutions in 2017.

NIS Directive mandatory incident reporting

Under the NISD, OESs (providers of services that are essential for maintenance of critical social or economic activities, such as services in the banking, energy, transport and health sectors) and DSPs (providers of e-commerce, search engines and cloud services) are required to notify their supervisory authority or the competent computer security incident response team (CSIRT) without undue delay of any incidents having – respectively – a significant or substantial impact on the service provided.

The competent authority or the CSIRT informs the other EU Member States significantly/substantially involved by the incident.

The deadline for national implementation of NISD is 9 May 2018. NISD is a minimum harmonisation directive and allows Member States fairly wide discretion in their implementation of its requirements. By way of example, as at the date of this briefing, various jurisdictions have taken steps to implement the NISD, including:

- **Italy**: The Government has issued a draft of legislative decree, subject to the Parliament's opinion. National strategy on the security of network and information systems has not yet been adopted. The Ministry competent for the operator's business sector is the NIS competent authority. Penalties up to EUR 120,000 (up to EUR 150,000 for non-compliance with instructions

specifically provided to an operator by the competent Ministry) will apply in case of non-compliance – these amounts can triple when the same breach is repeated.

- **UK**: The UK Government consulted on its approach to implementing the NISD in August 2017 and published its response to the comments received at the end of January 2018, although the final regulations implementing the NISD are still awaited. Of particular note, the UK proposes that the designated competent authority in each sector will publish relevant incident reporting thresholds before May 2018 and that competent authorities will be able to impose penalties of up to £17 million for breach of NISD requirements.
- **France**: The French NISD implementing law has been published on 27 February 2018. It will become applicable no later than 10 May 2018. However, the OESs will be designated by the French Prime Minister no later than 9 November 2018. Pursuant to this law, if an OES or a DSP does not comply with its obligation to notify severe security breaches which have (or, for an OES, which will likely have) a significant impact on the provision of the services, to the French National Authority of Information Systems Security (ANSSI), its managers could be personally subject to penalties of up to EUR 75,000 (in the case of an OES) and EUR 50,000 (in the case of a DSP).

  Please note that the French NISD implementing law will co-exist with the existing French military programming law on critical infrastructure information protection of December 2013 (CIIP Law) which covers similar topics but applies only to operators of "vital importance" (OVIs). Pursuant to the CIIP Law, OVIs must notify to the ANSSI all incidents affecting the operation or the security of their information system. Criminal fines of up to EUR 150,000 for executive managers of OVIs and criminal fines of up to EUR 750,000 for OVIs themselves (as legal persons) can be imposed.

eIDAS Regulation security incident reporting

Under the eIDAS Regulation, qualified and non-qualified trust service providers (TSPs) are required to notify their supervisory body without undue delay and in any event within 24 hours after having become aware of a security breach or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where applicable, TSPs should also notify other bodies, such as a data protection authority. If the breach is likely to adversely affect a natural or legal person to whom the trust service has been provided, TSPs must also inform them of the breach without undue delay.

SUMMARY COMPARISON TABLE

	GDPR	PSD2	NIS Directive	eIDAS Regulation
Who does the obligation apply to?	Data controllers (and data processors to notify controller)	Payment service providers	Operators of essential services / DSPs	Trust service providers, in relation to electronic identification schemes notified under the eIDAS Regulation
Trigger for notification	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data	Major operational or security incident, meeting one 'higher impact' or three 'lower impact' criteria	Incidents with a significant/substantial impact on the continuity of essential services or the provision of e-commerce, search engines and cloud services	Any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein
Timing of initial notification	Within 72 hours from the data controller being aware of the data breach (data processor must also notify controller without undue delay if aware of breach)	Within 4 hours from first detection	Without undue delay	Within 24 hours after having become aware of the incident
Notification to regulator required?	Yes, requirement for data controller to notify the GDPR home competent supervisory authority	Yes, requirement to notify the PSP's home competent authority	Yes, requirement to notify the NIS home competent authority or the CSIRT	Yes, requirement to notify the TSP's supervisory authority and other relevant bodies "if applicable"
Need to notify affected customers / individuals?	Yes, if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons	Yes, if the incident has or may have an impact on the financial interests of its payment service users	No (although regulator / CSIRT may inform the public)	Yes, if the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided
Ongoing notification / updating required?	No, although may provide information in phases	Yes, intermediate reports required at least every three days or whenever there is a new status update; final report to be submitted once root cause analysis carried out	No	No

	GDPR	PSD2	NIS Directive	eIDAS Regulation
Penalties for non-compliance	Fines for failure to notify ranging up to EUR 10 million or 2% of global turnover	Member States are required to have "effective, proportionate and dissuasive" penalties for breach of national laws transposing PSD2	Member States are required to have "effective, proportionate and dissuasive" penalties for breach of national laws transposing the NIS Directive	Member States are required to have "effective, proportionate and dissuasive" penalties for breach of the eIDAS Regulation
Application date	25 May 2018	13 January 2018 (for national implementation)	9 May 2018 (for national implementation)	1 July 2016

COMPARING REQUIREMENTS ACROSS REGIMES

Identifying incidents and breaches: protected properties and incident dimensions

When identifying whether or not any notification requirements are triggered, firms must first consider whether an incident has occurred falling within scope of one or more of the reporting regimes under GDPR, PSD2, NISD or the eIDAS Regulation.

The EBA guidelines on major incident reporting under PSD2 define an "operational or security incident" as an unplanned event or series of linked events that "*has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services*".

They also outline what is meant by each of these five dimensions that could be affected by an incident. The first four (integrity, availability, confidentiality and authenticity) are based on international standards and are also referred to in the ENISA guidelines under NISD, as "*the 4 properties or protection goals that a digital service must assure under the NISD*".

According to the guidelines on data breach notification under the GDPR, a personal data breach may be (i) a "Confidentiality breach" (in case of unauthorised or accidental disclosure of personal data or unauthorised access to such data); (ii) an "integrity breach" (in case of unauthorised or accidental alteration of personal data); or (iii) an "availability breach" (in case of accidental or unauthorised loss of access to personal data or destruction of such data).

While the notification requirements under the NISD do not apply to TSPs subject to notification requirements under the eIDAS Regulation, the NISD guidelines identify a potential overlap with GDPR notification requirements in relation to confidentiality breaches in particular, noting that DSPs may have to report the same incident under both NISD and GDPR. The guidelines highlight by way of example the 2011 Dropbox bug that allowed users to log onto the platform using only their username for several hours, due to a code update that suppressed the password authentication method.

Assessing significance of an incident or breach

Under PSD2, only "major" operational or security incidents need to be notified. The EBA guidelines set out various criteria and impact thresholds against which PSPs should assess incidents, providing that incidents should be classified as "major" where they meet one higher level threshold or three lower level thresholds.

Similarly, under the NISD and eIDAS Regulation, incidents are required to be reported only where they have a "significant impact" (or, with regard to DSPs, a "substantial impact") on the continuity of essential services (or the provision of e-commerce, search engines and cloud services, as regards DSPs), or on the trust service provided or personal data maintained therein, respectively. Again, the ENISA has developed guidelines under both the NISD and eIDAS Regulation explaining how firms should assess whether an incident has a significant impact.

Although there are some common themes for making these assessments, such as considering the number of affected users and the duration of an incident, each regime will require its own assessment to be made, against different criteria and thresholds in accordance with the relevant guidelines.

The GDPR does not include a significance threshold but instead requires notification of all personal data breaches, unless the breach is "*unlikely to result in a risk to the rights and freedoms of natural persons*" (Article 29 Working Party guidelines on personal data breach notification).

In addition, the GDPR requires information to be provided to individuals when "*the personal data breach is likely to result in a **high** risk to the rights and freedom of natural persons*" (Article 29 Working Party guidelines on personal data breach notification). This requirement does not apply when appropriate organisational measures to neutralise the risk have been implemented or communication to individuals would involve disproportionate effort (in this event, public communication or similar measure are required).

Notifying competent authorities

The EBA guidelines under PSD require PSPs to submit the initial notification within four hours of becoming aware of a major operational or security incident, as well as providing intermediate status update reports and a final report once root cause analysis has been carried out. This is significantly shorter than the 24 and 72 hour deadlines under the eIDAS Regulation and GDPR respectively. The NIS Directive is less prescriptive, requiring operators of essential services to notify the competent authority or CSIRT "*without undue delay*".

In addition, only the PSD2 regime requires formal ongoing notification requirements in the form of intermediate and final reports, although GDPR expressly provides that a data controller may provide information in phases where not initially possible to provide all required information. More generally, competent authorities may of course request further information as part of any investigation into an incident.

The regimes also identify different competent authorities to whom reports should be submitted and associated guidelines provide for different reporting templates and information.

Notifying affected users, individuals or the public

The GDPR, PSD2 and eIDAS Regulation also require firms to notify affected users or individuals of incidents in certain circumstances. Broadly, this is required where the incident has or may have an impact on the user or individual in question, although each regime includes its own test as to when such notification is required. Whilst GDPR is concerned only with personal data of natural persons, the user notification requirements under PSD2 and eIDAS may also apply to legal persons that are affected by the incident or breach.

There is no requirement under the NISD for DSPs to notify affected users or individuals of an incident, but the competent authority or the CSIRT may inform the public about individual incidents, after consulting the notifying operator of essential services, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.

Similarly, a supervisory body should inform the public of an incident under the eIDAS Regulation (or require the TSP to do so) where it considers this to be in the public interest.

Glossary

CSIRT – computer security incident response team

DSP – digital service provider

EBA – the European Banking Authority

ECB – the European Central Bank

eIDAS Regulation – the Regulation on electronic identification and trust services (910/2014)

ENISA – the European Union Agency for Network and Information Security

GDPR – the General Data Protection Regulation (2016/679)

NISD – the Network and Information Security Directive (2016/1148)

OES – operator of essential services

PSD2 – the recast Payment Services Directive (2015/2366)

PSP – payment service provider

PSU – payment service user

SSM – the Single Supervisory Mechanism

TSP – trust service provider

CLIFFORD

CHANCE

CONTACTS

Peter Chapman
Senior Associate

T +44 2070061896
E peter.chapman
@cliffordchance.com

Laura Douglas
Professional Support Lawyer

T +44 207006 1113
E laura.douglas
@cliffordchance.com

Carlo Felice Giampaolino
Partner

T +39 064229 1356
E carlofelice.giampaolino
@cliffordchance.com

Jérémy Guilbault
Avocat

T +33 14405 2480
E jérémy.guilbault
@cliffordchance.com

Jonathan Kewley
Partner

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

Dessislava Savova
Partner

T +33 14405 5483
E dessislava.savova
@cliffordchance.com

Alessandro Sciarra
Lawyer

T +39 064229 1384
E alessandro.sciarra
@cliffordchance.com

Samantha Ward
Senior Associate

T +44 207006 8546
E Samantha.ward
@cliffordchance.com