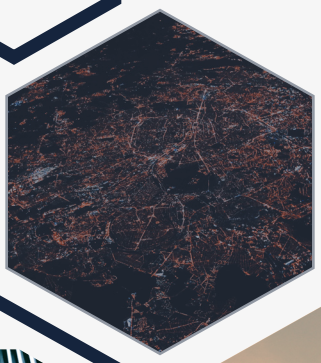
HOLLAND FINTECH

Introductory Guide:

Key Issues in Cybersecurity and GDPR Compliancy



A collaborative introduction to the key cybersecurity trends that are facing the financial services industry, with tips and tricks from experts in the field on how to mitigate these risks and ensure compliancy.

Qbit CYBER SECURITY · eurofiber · CyNation · INNOPAY · GINGER · intermax

Table of Contents

Introduction

Personal data protection risks

Mathijs Hummel, QBIT

Technical Considerations

Increasing cybersecurity: Granularity and encryption levels

encryption, tokenization, key management systems, granularity, cryptoshredding

Maarten Sander, Ginger

Cybersecurity: At the infrastructure and network level

data storage, data transport, information requests, physical network security

Paul Teixeira, Eurofiber

Practical Considerations

Security as the foundation of digital trust

security and market dynamics, how to: improving digital trust

Jelger Goenland, Innopay

A shifting paradigm: From data privacy to data risk management

consumer sentiment, embedding privacy, how to: developing privacy framework

Shadi Razak, CyNation

Organisational Considerations

GDPR stimulus: Managing cybersecurity priorities

security awareness, assigning responsibility, outsourcing tools

Ludo Baauw, Intermax

Assessing your organisational vulnerabilities: GDPR and cybersecurity

organisational processes, assigning responsibility, organisational assessment

Mathijs Hummel, QBIT

Introduction: Personal data protection risks

Mathijs Hummel, Privacy Advisor

Qbit
CYBER SECURITY

GDPR demands the safeguarding of data subjects' rights and interests. It allows for organizations to employ a risk based approach to personal data protection. This means that organizational risks and interests may be weighed against a data subject's rights and interests. Subsequently, both organizational risks, as well as data subject risks need to be taken into account when assessing whether the processing and protection of personal information is performed adequately. Due to the contextual nature of privacy, different situations will lead to risks and interests being weighed differently, depending on each individual situation. Notable risks and threats are found outside, as well as within the organization.

As crime is shifting from the physical world to the digital world, so are the methods utilized. Ransomware and social engineering (CEO-fraud for instance) are methods readily available to criminals.

> *"The attack surface is large, the chance of getting caught is small. The impact and damages caused by ransomware, as well as social engineering can be loss of information, information leakage or perhaps the inability to access and use information."*

The SWIFT-hacks that took place in 2015 and 2016 are major examples. Add personal information to the mix, and the results are data breaches; possibly adding fines, penalties and loss of public image to the list of risks and effects.

Looking at internal risks, technical vulnerabilities and a lack of employee awareness is lurking in the shadows. Undetected technical vulnerabilities will expose infrastructures, systems, organizations and (financial) information to outsider threats. These are becoming increasingly more dangerous the longer they go unnoticed. Employee awareness is key to preventing or combatting social engineering and ransomware. GDPR acknowledges this, as it directly states that measures need to be taken to increase employee awareness, as well as putting time and effort into employee education.

There is one last risk left unaddressed: when data protection is not properly incorporated in business processes. Principles such as privacy by design, data minimization, transparency etc. all need to be addressed in one form or another. The lack of proper and timely incorporation of these principles throughout an organization, will ultimately lead to inefficiency and stagnation, but more importantly, negatively influence the processing of personal information and therefore negatively impacting the individual whose personal information is being processed.

Increasing cybersecurity: Granularity and encryption levels

Maarten Sander, Managing Partner

GINGER

Ginger is a Payments as a Service Platform that builds, improves, reroutes, or replaces the payment technology of banks, other financial institutions and fintechs.

When servicing financial institutions (FI's) with its complete end-to-end Payments-as-a-Service platform, Ginger often receives requests to give advice on how FI's can increase their cybersecurity and reduce the risk and impact of data breaches. With a simple and clear roadmap, FI's can secure their data and reduce their cost of compliance.

Firstly, FI's should encrypt all personal data, both in transit and at rest. When sending or receiving personal data, make sure that the connection or the data itself is encrypted. This ensures that the information cannot easily be intercepted. Encrypting the personal data when stored on disk or in a database prevents visibility in case of unauthorized access.

ENCRYPTION AND THE GDPR

Firms are specifically required to implement risk-based measures to render personal data unintelligible to anyone not authorised to view it - one such measure is personal data encryption.

Secondly, we advise to use a centralized key management system. This will allow for more convenient development of company-wide encryption policies and processes that scale with your organization. Centralizing all key management is also a good first step towards automating these processes.

Additionally, for highly sensitive data (e.g. credit card numbers or IBANs), consider tokenizing the information. Tokenization allows you to centralize the protection of sensitive data in a data vault, reducing the impact on many business processes and reducing the scope of your PCI-compliance. Global financial services companies trust Ginger's off-site tokenization solution for the storage of sensitive information. This service will allow you to be GDPR compliant and improve the protection of highly sensitive data, without incurring high costs and burdening your IT organization.

TOKENIZATION AND THE GDPR

As the GDPR calls for data security measures appropriate for the level of risk presented by processing certain personal data points. As tokenization is one of the most secure measures, pseudonymizing data this way may lead to not only compliancy but may facilitate the processing of personal data beyond the original collection purposes.

> *"Businesses must consider the granularity of encrypted data."*

Would it make sense for your business to encrypt a full customer object, its individual fields, or perhaps it is more efficient to encrypt these fields combined into logical groups? This depends on business and regulatory requirements. More granular encryption allows for more control over when to remove encrypted data.

GRANULARITY AND THE GDPR

Granularity refers to the scale or level of detail in a dataset. This is particularly relevant for the data minimization principle which calls for periodical reviews of stored personal data .

Firms must take into consideration the granularity of encrypted data to ensure they have adequate control over distinguishing, separating and erasing particular data points. The ICO gives the example that a Debt collector searching for a debtor, need only keep the minimum amount of data needed to form basic identification of people they have removed from their search, and any additional information should be erased. In this case the FI must be able to erase the part of the customer's personal data that has become unnecessary, but keep the relevant data points

Firms must also take into account the means of which they are erasing data, using techniques like crypto-shredding.

CRYPTOSHREDDING AND THE GDPR

Crypto-shredding refers to the deliberate deletion or overwriting of the encryption keys required to unlock data, rendering it unreadable. As the GDPR calls for timely erasure of personal data upon valid request, firms must ensure they are able to put that data 'beyond use'. Oftentimes even where data is erased off live systems, it can exist in the backup environment until overwritten. However, with crypto-shredding, that data is immediately placed beyond use when the encryption key is destroyed.

Cybersecurity: At the infrastructure and network level

Armijn Spreitzer, Products Manager

eurofiber

Eurofiber operates high-quality digital infrastructures, with their own open fiber optic network and data centers. They offer companies, governments and non-profit organizations future-proof, smart solutions to enable cloud computing, organisational agility and GDPR compliant encryption.

ADDRESSING GDPR: START AT THE NETWORK LEVEL

Data is rapidly becoming the lifeline of organisations and governmental institutions. The free flow of digital information ensures that companies and governments alike can function without a glitch. With the advent of the GDPR, it's not enough to have that data collected and stored in a secure manner. The transport of the information itself has to be secure as well. And the data has to be available at any time, in order to, for example , ensure that information requests of citizens can be met. These are, unfortunately, parts of the GDPR that haven't garnered a lot of public attention.

Ensuring that your network connections are as secure as possible is an important factor in complying with the GDPR. Securing data and ensuring that access to that information is unhindered starts at the network level.

INFORMATION REQUESTS UNDER THE GDPR

In this case 'unhindered access' refers to data subjects' right of access. Data controllers (in most cases) have one month to respond to such a request, with subjects able to demand a copy of their personal data, the purpose of its processing, its reciepents, and the duration of retention (not definitive).

> *"Cybercriminals and hackers can strike during the transport of data to and from data collection points and data centers. For example, by using 'the man in the middle methods' or simply by electronically eavesdropping on the network connection itself."*

PHYSICAL NETWORK SECURITY

Modern network connections, provided by fiber optic networks, can be secure by nature. The fiber optic network of Eurofiber - a leading fiber optic network provider in The Benelux – is a good example. All the Eurofiber network cables are to be found underground, making them virtually inaccessible for third parties. A potential weakness of a fiber optic infrastructure is the connection to the 'normal' network, for example in a company building. Eurofiber welds those connection points, instead of connecting them in a normal way, making data tapping virtually impossible.

ENCRYPTION

In order to have an even higher level of security in the network connections, one can have data encryption on the network level itself. In the world of fiber optics, this is the so called 'Encrypted Wave Dimension Multiplexing'. This service encrypts all data during the physical transport from A to B on a basic network level.

REDUNDANCY

The second aspect of the GDPR requirements, the availability of data, can also be achieved at the network level. For example by ensuring that the physical cables are installed underground. And by having so-called 'redundant connections' disruptions in the network can be addressed instantly without the flow of data being hindered.

In short: providing the security and maximal availability of data at the network level addresses a substantial part of the GDPR.

Security as the foundation of digital trust

Jelger Groenland, Digital Trust & Security

INNOPAY

Europe, not the United States, is where the future of tech companies will be determined. As part of their vision for the digital single market, the European regulator is introducing new legislation to empower customers. It gives consumers control over their data, empowers them to protect their privacy and how their data is monetised. This raises awareness with the general public about the value and risks associated with their data. It raises questions in the mind of the customer about how well companies are protecting their data and if they can be trusted. GDPR was only a start, the debate has moved beyond compliance.

Data is the differentiating raw material for the digital economy. All successful organisations have a data driven strategy or are working to develop one. This means figuring out an approach where business models, processes and services are based on data insights about customers and markets. This means organisations are collecting large quantities of data and store it with the intension to leverage it as a competitive advantage.

> *Achieving trust is not an easy objective. It should be approached strategically as it is a long-term necessity for businesses.*

Regulators are taking notice. Especially in the EU, driven by the vision of a digital single market, new regulations on digital trust and data security have been introduced. The EU effectively leading the way in regulating the digital markets with regulations like eIDAS, GDPR, NIS Directive, the ePrivacy directive, PSD2 and others. It requires organisations to be more careful with customer data and empowers customers to demand their rights as digital citizens. Questions are raised about value of data and the risk of loss or mis-use. Consequently, customers demand more control over their personal data and how data is being used. They demand a fair value exchange, where there is a balance in the benefits organisations and individuals get from this data.

HOW MARKET DYNAMICS ARE INCREASING THE NEED FOR DIGITAL TRUST

Customers have become more critical about who to trust their data, influencing buying decision. Several studies found that robust security practices are influencing buying behaviour due to the trust it provides to end customers. A study published in Harvard Business Review shows that consumers in mature markets, like the EU, let their buying decision influence by how much they trust an organisation or platform. Leading organisations need to demonstrate they can be trusted – by investing in security, being transparent about data usage, give customers control, ask for consent and build accountability into business model. At the same time the digital attack surface of the organisation is widening. As everyone needs access to everything at any time, more connections, and data assets need be protected. Leveraging technology and innovative data models has become a competitive advantage, but risk of poor selection and/or building technical debt has risen significantly as well. This makes it increasingly important to invest in security strategically.

WHAT BUSINESSES CAN DO TO IMPROVE DIGITAL TRUST

There are several strategic initiatives an organisation should pursue to become more trusted, including the following:

Start with a digital trust strategy Build a digital trust strategy and embed this into your organisational processes and products. Start with the customer value proposition and their perspective on security. Make this the core of your digital trust strategy.

Share insights and collaborate in cyber coalitions To face the ever-increasing threat, companies need to collaborate and share data with other organisations. This can be done via industry Information Sharing and Analysis Centres (ISAC) for instance or via other bilateral agreements and cyber coalitions. It does however require robust agreements on how risk and threat data is being shared and used.

Customer onboarding and authentication Build a customer onboarding and authentication capability which is both seamless and secure. Knowing your customer across multiple channels, offering secure ways to communicate, and empower the customer to control their data is needed to build a meaningful and trusted relationship.

Data privacy: A shift from regulatory compliance to risk management

Shadi Razak, CTO

CyNation

Privacy risks are about the impact on an individual when information about them is processed in applications and systems. Such risks may materialize first and foremost in data breaches, but also in (other) situations where personal data can be accessed without authorisation, or used without a connection to predefined purposes.

Until recently privacy was treated in a similar way to security 10 years ago: it was bolted on after the fact instead of being embedded into day-to-day operations. This is clearly inadequate: data privacy is not just about GDPR or one particular regulation. Organisations operating or offering their services and products globally, such as many Fintech start-ups, are confronted with multiple overlapping data protection and privacy laws and standards that they must adhere to and comply with. This is why it is imperative to promote privacy principles throughout the entire organisation. However, the underlying reason should go beyond regulatory compliance and focus on practical privacy risk management throughout the entire data life cycle; leveraging this as a competitive advantage.

IMPORTANCE OF EMBEDDING PRIVACY PRINCIPLES

Just because an organisation has a user's data, or a way to obtain it, doesn't necessarily mean they should use it. In recent years various studies have shown that valuing customers means valuing their privacy. Privacy risks matter to businesses because the individuals whose privacy they guard are their employees, customers, patients, consumers, citizens etc. If individuals see their personal privacy violated, this may severely test their loyalty to their employer, make them less likely to purchase from a particular vendor, or less likely to trust their healthcare provider. In other words, privacy risks have clear, measurable business impacts on revenue growth, net profit margin, customer satisfaction and earnings per share.

In addition, privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organisation's default mode of operation. Embedding privacy principles into the organisation operation and data life cycle will minimize the risks to the individuals. The risk of non-compliance will decrease, while trust in the organisation and its reputation will increase accordingly. On the other hand, if the risk to the individual is not addressed, or it actually increases, the overall risk to the business will also increase, along with reputation damage and lack of trust in the business.

HOW TO EMBED PRIVACY: PRIVACY RISK MANAGEMENT

While privacy risk management does not defeat regulatory rights or obligations, nor remove organisational accountability, it is a valuable tool for calibrating the implementation of and compliance with these privacy requirements, whilst building trust and gaining the loyalty of various stakeholders. Effective privacy risk management should include a practical framework that maintains a balance between strategic business objectives and privacy obligations based on the actual risks and benefits of the proposed data processing.

DEVELOPING PRIVACY RISK MANAGEMENT FRAMEWORK

Checklist: Your framework should...

- Identify and classify the different datasets collected and processed across the organisation.
- Assess and prioritise the business risks of mishandling or losing any of the business-critical datasets.
- Define data privacy and protection policies, standards, and guidelines that detail the business, technical and security requirements to support data privacy assurance and strategic business risks mitigations.
- Assign roles and responsibilities of the different stakeholders, and establish clear principles of accountability.
- Support: from the organisation's top management. In turn they will manage and ensure the different stakeholders' (teams and departments) participation in the development process.

CyNation provide an automated risk management platform, CyDesk, providing organisations with real-time visibility of their risk exposure and actionable intelligence to manage their risk, including:

1. Realise and classify sensitive and critical datasets across the organisation.
2. Verify that all personal data processed on individuals (clients and employees) should be correct, accurate, relevant and serve a purpose.
3. Openness: make individuals are aware of what personal data about them is processed, on which grounds and for what purposes.
4. Minimise: data retention periods that are only as long as necessary, and as short as possible.
5. Protect: personal data by defining practical security controls and measures to adequately assure the privacy and security of such data as long as it is in existence.

GDPR Stimulus: Managing cybersecurity priorities

Ludo Baauw, CEO

intermax

In general we notice that the GDPR has raised awareness of the importance of information security. People are more conscious about what happens with their data, and more and more companies take steps to improve or establish their information security policy. We also see more companies understanding the importance of defining the responsibilities in this area. All these developments not only help companies complying with new legislation such as the GDPR, they also help them prove to their clients that their data is safe with them.

> *"However, there's also a certain kind of confusion that has sometimes led to a passive attitude in the market, caused by the enormous amount of new suppliers we've seen since the introduction of the GDPR (that offer even more new tools)."*

As a result of this situation companies seem to sometimes lose sight of their needs in this area and end up not taking any action at all. Also, a lot of these new tools address only part of the problem at best.

FOR INSTANCE...

Take SIEM (Security Information & Event Management, ed.) for example, a sometimes very expensive solution that often leaves companies with a huge amount of data that they then can't investigate or follow-up, due to a lack of resources. SIEM is also very much a future-oriented tool, and we always advise companies to start with a thorough assessment of their current situation in the field of information security.

Your information security management program should be based on the implementation of certain processes within your organization. Once that base is established, you can look further to see if and what tools you might need to improve your program. This really doesn't have to cost an enormous amount of money.

DATA BREACHES

We encourage our clients to take several steps to protect themselves from data breaches. First, you have to register the kinds of data you process within your company and map out where what data is. With this information you can start putting measures into place to protect your data, and – very important – monitor the effectiveness of these measures. This serves as valuable input to constantly improve your information security management program.

It is important for companies to realize that many data breaches are - often unintentionally - caused by their own employees; after all, they're the people working with the data. It is therefore essential to train your people on increasing their awareness around this matter - security awareness training sessions and phishing and social engineering tests are excellent ways to accomplish this - and to establish clear rules, responsibilities and processes for them. These for example can include assigning a security officer and data owners, and carefully registering all incidents. It's also important to create a culture where employees feel free to report security incidents. All of these things offer valuable input on how to further improve your information security policy.

ASSIGNING A DPO AND THE GDPR

While important to have clearly established roles and responsibilties for various data, some firms under the GDPR are additionally required to appoint a Data Protection Officer. They are tasked with monitoring compliance with the GDPR and other data protection laws, awareness-raising, training, and audits. They must also report to the highest level of management.

REGISTERING SECURITY INCIDENTS AND THE GDPR

Those subject to the GDPR must keep a register of all security incidents and data breaches within the firm, and report data breaches to the DPA within 72 hours of discovery. Additionally, data subjects must be informed when it is likely that the data breach will result in a high risk to their privacy.

Financial services companies should keep in mind the speed with which the market of information security is changing. It's getting harder and harder for these companies to protect themselves against actual threats as they change and evolve daily, and at the same time to maintain compliance with new legislation and other developments, such as the introduction of PSD2. There just aren't enough resources and manpower in the financial market itself. Outsourcing IT infrastructure to service providers where security forms part of their core business and who are extensively certified by independent auditors is therefore advisable. This allows firms to rely on up-to-date knowledge and tools, showing your customers that you take information security seriously. After all, it can be catastrophic for fintech companies if something goes wrong and they get to deal with serious data breaches.

GDPR and cybersecurity: Assessing your organisational vulnerabilities

Mathijs Hummel, Privacy Advisor

Qbit
CYBER SECURITY

When dealing with personal information under GDPR, it is not stated explicitly what specific measures need to be taken by an organization to constitute 'adequate protection'. Instead, a more abstract and high-level approach is employed, resulting in room for interpretation. This may seem difficult to grasp at first. A common mistake is to take an approach that is too restrictive and therefore detrimental to both the organization and the individual of whom personal data is processed, even though the exchange of information is meant to safeguard a different interest for that individual. This may lead, for instance, to restricting the exchange of financial information to a third party, whereas the exchange is aimed at benefitting the individual the information refers to. These pitfalls are prevalent throughout many different sectors and employing an approach that is too restrictive will ultimately harm individuals more than it aims to protect them. I want to reiterate that privacy is important, but not absolute. It becomes even more important when taking into account legislative developments such as PSD2, which appear to directly contradict the principles in the GDPR.

DIVIDING ORGANISATIONAL RESPONSIBILITY

> *At Qbit, we believe that GDPR presents opportunities for organizations that incorporate privacy principles from the outset and by doing so increase their operating efficiency, gain a competitive advantage, reduce risks for individuals as well as improve their public image.*

The distribution of privacy and security responsibilities throughout all organizational layers plays an important part in using data protection to your advantage. Adequate protection can be divided into three areas: organizational, technical and human. Measures taken will affect one or more of these areas. Effectiveness is however highly dependent on human action. Employee awareness is paramount, as a lack of awareness may result in circumvention of technical measures, or delays in breach notification. Focusing equally on the organizational, technical and human aspects of privacy is essential to take control of personal data protection.

ASSESSING YOUR CYBERSECURITY VULNERABILITIES

Improving personal data protection starts with assessing your current situation. What types of personal data are processed and to whom does it refer? Then proceed to analyse current measures taken to protect the personal information. Take into account organizational, technical, as well as human measures. This gives you an overview of the current situation. Next, take on the perspective of the data subject(s) involved and ask yourself critically: Am I doing enough to protect the individual's interests, or should I do more? If you feel you should do more, are there valid arguments to balance this against a different interest? If not, that is where you should improve.

> *It is important to note, that personal data protection is not a onetime effort. Continuous protection depends wholly on re-evaluating a situation periodically.*

By understanding this, you can prevent blind spots that otherwise may have led to exploitation of vulnerabilities, or falling victim to social engineers, resulting in data breaches or significant losses.

QBIT

At Qbit, we specialise in helping organisations take control of privacy protection and cyber security. Our services are structured around the three pillars previously mentioned. We employ experts in the fields of technical security, human awareness, it-auditing and compliance. Our services range from compliance checks, risk assessments and legal advice, to audits, technical security assessments and social engineering. We also provide our Data Protection/Security Officer-as-a-service, to perform DPO-, or security officer-duties for our clients, and manage incident response in the case of data breaches or security incidents.
Our mission is to ensure that each of our clients can recognise, prevent and defeat cybercrime and other threats. We take organizations by the hand, are convincingly innovative and progressive and at the same we time we are honest and approachable.