
# PROTECT YOUR DATA AND PREPARE FOR THE EUROPEAN **GENERAL DATA PROTECTION REGULATION**

NRB

DARING TO COMMIT

# INSIGHTS

The EU's new data protection regulation, known as the GDPR (General Data Protection Regulation), can impact your organisation significantly in terms of how to handle personal data. Your organisation will not only be responsible for ensuring compliance with the regulation in terms of handling and protecting personal data, it could even be penalised for non-compliance and it will be liable for any damage resulting from data breaches.

NRB provides expertise in GDPR and has developed a modular approach supported by a portfolio of services to guide you towards GDPR compliance at your own pace taking into account your organisation's security maturity and your budgetary means.

# ABOUT **GDPR**

The General Data Protection Regulation wants to harmonise the data protection regulations throughout the EU and to strengthen and unify data protection. It addresses personal data security for EU citizens and individuals within the EU, but regulates also export of personal data outside the EU. The Commission's primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The GDPR was adopted on the 27th of April 2016. It enters into application on the 25th of May 2018 after a two year transition period and will replace the current data protection directive 95/46/EC from 1995. Unlike a directive, it does not require any enabling legislation to be passed by governments.

# WHY YOU SHOULD GET PREPARED FOR THE NEW REGULATION?

The GDPR will supersede all current national data protection laws in the EU. Here is an overview of the main expected changes that organisations will have to be aware of and adapt to:

### Expanded territorial reach:

The GDPR applies to organisations and their sub-contractors outside the EU. This means in practice that a company outside the EU, that is targeting consumers in the EU, will be subject to the GDPR.

### Accountability and Privacy by Design:

The GDPR makes organisations fully accountable for demonstrating compliance. This includes requiring them to document compliance, conduct data protection impact assessments for risky data processing and implement data protection by design and by default in their operational processes.

### Consent:

A data subject's consent to processing his or her personal data must be given freely, and for sensitive data explicitly, either by a statement or a clear affirmative action stating agreement to the processing. Consent can be withdrawn at any moment. The organisation is required to be able to demonstrate that consent was given.

### Data Breach Notification:

Organisations must notify data breaches to the Data Privacy Authority. This must be done without delay and, where feasible, within 72 hours of awareness. A substantiated justification must be provided if this timeframe is not met. The organisation must notify the affected data subjects without delay when their data has been compromised.

### Role of subcontractors:

One of the key changes in the GDPR is that sub-contractors have direct obligations. This includes implementing technical and organisational measures and notifying your organisation without delay of data breaches.

### Sanctions:

The GDPR establishes penalties for breach imposing fines for infringements of up to 4% of annual worldwide turnover on data breach and up to 2% of annual worldwide turnover on non-compliance.

### Data Protection Officer (DPO):

In specific circumstances organisations or subcontractors must designate a Data Protection Officer. The DPO will need sufficient expert knowledge. The DPO may be employed or under a service contract.

### Right to be forgotten:

Individuals can require their personal data to be erased without undue delay by the organisation. A good example is where they withdraw consent and no other legal ground for processing applies.

# **9 STEPS GUIDE** ON HOW TO GET STARTED WITH GDPR

- **Key to success towards GDPR compliance is stakeholder buy-in.** Start with creating an urgency at director or board level. Key stakeholder buy-in at C-level is a critical success factor to engage the necessary resources and to have GDPR compliance on the right position within the corporate priorities.

- **One of the first steps in the actual data protection is knowing where your data resides.** Perform a data identification, ideally a combined exercise of manual interviews and automated data crawling. Once data is identified properly classifying, labelling and tagging data is a prerequisite towards defining a clear scope for your GDPR compliance gap analysis and compliance program.

- **Collaboration between IT and legal is critical.** The regulation does not provide exact definitions that can be applied out of the box. Interpretation, risk assessment, legal backing and corporate level decision will be necessary all the way.

- **Stakeholder management is necessary throughout your entire enterprise.** Creating a minimum of awareness and understanding about the regulation will raise the required attention and collaboration from the different business units. Awareness is not a one-time shot. Make awareness an integrated part of your compliance program and repeat sessions and campaigns at regular intervals.

- **Appoint a responsible for GDPR compliance.** Whether your organisation is subject to the obligation of appointing a DPO or not, it is advised to assign a responsible that oversees the compliance track towards May 25, 2018 and assures continued compliance once GDPR becomes in effect.

- **Align your GDPR compliance and data protection track with a security framework such as CIS, ISO27001, NIST, … and integrate it in your security strategy and roadmap.** International organisations should also keep their branches and subsidiaries in mind. Each country has its preference in terms of framework and different governments require different frameworks. Compliance framework mappings do exist and can be helpful to develop a global compliance approach.

- **Base your data protection strategy and roadmap on a risk assessment.** Protecting your personal data at 100% is simply impossible and attempting to, will saddle you with an enormous cost and effort. Concentrating on the most pressing topics will give you quick benefits and provide focus.

- **Perform a GDPR compliance gap analysis, optionally combined with a data protection or security maturity assessment.** In combination with a risk assessment this gives you all necessary information to establish a multi-year data protection and security roadmap with strong justified foundation.

- **Data classification, installation of data protection and governance is not a one-time shot.** Ensure the implementation of policy through automated data protection enforcement, specifically for sensitive or personal data. Hence the need of clear accountability at director level and a governance structure piloted by a Data Protection Officer or equivalent.


STEP 1
CREATE STAKEHOLDER BUY-IN
STEP 2
DO A DATA IDENTIFICATION EXERCISE
STEP 3
GET LEGAL & IT TOGETHER
STEP 4
RAISE AWARENESS
STEP 5
APPOINT A DPO (OR EQUIVALENT)
STEP 6
ADOPT A SECURITY FRAMEWORK
STEP 7
PRIORITISE THROUGH A RISK ASSESSMENT
STEP 8
PERFORM A GAP ANALYSIS
STEP 9
IMPLEMENT AUTOMATED ENFORCEMENT
GDPR

# HOW NRB **CAN HELP YOU**

- **Advisory services:** NRB can assist in roadmap design and strategic development for data protection through **consulting** or through staff provisioning at different levels. Our team of experienced consultants provides services from technical data automation to C-level advisory to ensure continuity and single accountability.

- **DPO resources:** many organisations do not have the required resources or competences to staff a Data Protection Officer. NRB provides individuals with the required competences and certifications to assist organizations in their GDPR compliance track in a **DPO, CISO (Chief Information Security Officer) or other role**, in project mode or in operational mode. The consultant can ensure all DPO responsibilities and can assist the organisation on a broader security context in a dedicated, shared, full or part time mode. If required, NRB can accompany the DPO with legal assistance through a recognised law firm to ensure legal advice.

- **Awareness campaigns:** they are key to success towards GDPR compliance. NRB does not only provide awareness sessions concerning the GDPR requirements, but extends awareness programs with practical sessions looking into the impact on business processes and daily operations. In addition, awareness programs are focused towards acceptance of change with the objective to not only raise awareness about data privacy but also towards the necessity of the GDPR compliance program.

- **Program and project management:** will be key throughout your entire data protection lifecycle. Whether you need a program manager to drive the compliance track on a high-level or you need a technical project lead to implement an automated solution, NRB provides resources with broad security competences, organisational and communication skills who are used to drive strategic change programs.

- **Risk assessment services :** NRB is experienced in risk assessment services which can be performed either with a broad scope towards enterprise IT security risk either with a limited scope specifically towards data protection or GDPR compliance. A risk prioritisation and impact analysis provides your company with an excellent tool to decide on your future investments, strategy and roadmap.

- **GDPR compliance assessment:** is a focused way and a short track towards identification of compliance gaps and can be a tool where budget is limited and resources are scarce. NRB executes a **Quick GDPR compliance assessment** to identify the areas where an organisation is not compliant. A high-level prioritisation can be defined in order to develop a compliance roadmap.

- **Automated data classification and protection:** a critical step towards GDPR compliance is the identification and classification of data. NRB provides leadership and expertise in **data classification** through a combination of manual and automated methods to ensure a full coverage. Data Classification is a highly interactive exercise in collaboration with the client stakeholders, which are significantly involved in the decision making process. NRB partners with different organisations such as **Varonis**, **Microsoft** and others to **automate data classification and data protection**. Through automated classification and data protection NRB ensures reduced project- and implementation costs. By enforcing and delegating policies, operational data management costs can also be significantly reduced.

- **Staff provisionning:** NRB can provision security staff at different levels.

# OUR SERVICES **FOR GDPR**

- ADVISORY SERVICES
- DPO RESOURCES
- AWARENESS CAMPAIGNS
- PROGRAM & PROJECT MANAGEMENT
- RISK ASSESSMENT SERVICES
- GDPR COMPLIANCE ASSESSMENT
- AUTOMATED DATA CLASSIFICATION AND PROTECTION
- STAFF PROVISIONING

# OUR **UNIQUE SELLING POINTS**

- ONE-STOP-SHOP CYBERSECURITY SOLUTIONS
- DEDICATED METHODOLOGIES FOR IMPLEMEN-TATION
- PRODUCT & VENDOR INDEPENDANT

# OUR **KEY DIFFERENTIATORS**

- NRB can rely on a rich pool of resources, covering a very broad range of security services from very technical competences to C-level advisors. Having a competent team of experts at its disposition is a major advantage that not many organisations can provide. NRB prefers to service you with the most 'fit for purpose' experts within a diverse project team to maximise the right expertise at the right level at the right time.

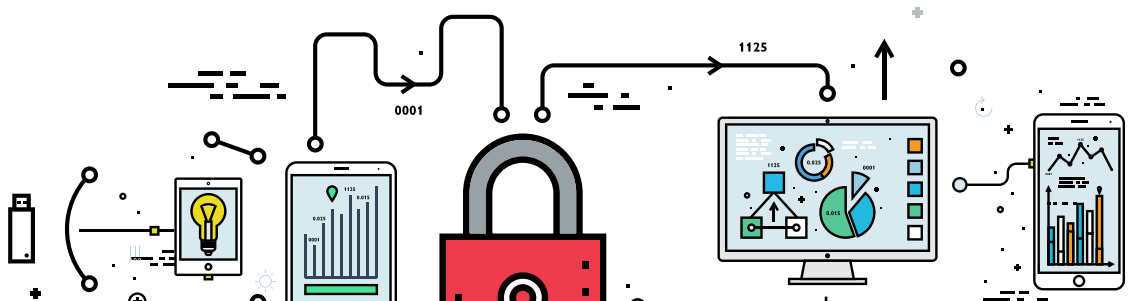
- Our client base extends throughout all sectors on a national scale. We have worked with a broad spectrum of organisational cultures and maturity levels. This experience gives us an empathic touch which is crucial to succeed in implementing strategic change within an organisation. Our approach is well-structured and methodological, but flexible and adapted to your organisational needs, to your organisation's capacity to change and to the objectives set by your management.

- Since the acquisition of Trasys, late 2015, NRB has become the largest national IT service provider. Our relations with vendors and partners extend beyond national boundaries and provide an unmatched pool of expertise, product support and competences. NRB is de facto a services company and is product and vendor independent. With our service-approach backed-up by our partnerships we are able to provide you with an independent advice on automation solutions and we offer a vast range of product implementation services with our own people or through our partners.

# NRB **SECURITY PRACTICE**

CyberSecurity is more than a few new products or gadgets. It's about a complete, integrated mind set, involving both proactive and reactive measures, people, processes and technology. CyberSecurity is also about understanding the business and aligning any project to the critical assets of the organisation. It is about monitoring, testing, building and maintaining a process and about creating a platform that lets you truly manage your risks in a world where the cost and damages of breaches continue to rise.

The NRB team of Information and CyberSecurity professionals plays the key role of trusted advisor to help the customer achieve his objective: connecting security to business agility. Our experts base their approach on the NIST (National Institute of Standards) and ISO (International Organization for Standardization) Cybersecurity frameworks for best practices. The main advantage of the NIST and ISO approaches consists in using business drivers to guide CyberSecurity activities and in considering CyberSecurity risks as part of the organisation's risk management processes. Our extensive portfolio of solutions and services can strengthen the prevention and management of CyberSecurity for critical data.



## GRC & TRAINING

- G – Security Governance
- R – Security Risk Management
- C – Security Compliance
- ISO 27001 Audit & Implementation
- IT Security Strategy & Roadmap, CIO/CISO Advisory
- Industrial Control Systems (SCADA) Security

PECB When Recognition Matters

## INFORMATION & DATA SECURITY

- Data Security Governance
- Data Classification
- Data Privacy & Protection
- General Data Protection Regulation (EU–GDPR)
- Data Leakage Protection Data Leakage Detection

Microsoft

## IDENTITY & ACCESS MANAGEMENT

- Identity Access Governance
- Identity Access Management
- Web Access Management
- Single Sign–On
- Privileged Account Security

BRAINWAVE

evidian

FORGEROCK

## INFRASTRUCTURE & APPLICATION SECURITY

- Infrastructure Security Architecture
- Firewall Management
- Penetration Testing
- Vulnerability Scanning
- Ethical Hacking
- Endpoint Security
- Application Security Testing

MaaS360 by Fiberlink, an IBM company

algosec

## SIEM & SECURITY INTELLIGENCE

- Security Incident & Event Management
- Security Operations Center
- Security Threat Intelligence

IBM QRadar


## Kris **Vansteenwegen**

Head of Security

e. kris.vansteenwegen@nrb.be
m. +32 (0)470 20 71 10



## Charles **Delhaye**

Consulting Division Executive

e. charles.delhaye@nrb.be
m. +32 (0)499 05 85 84


TRASYS
WE GET IT DONE

PART OF THE NRB GROUP

(*) Trasys Group is part of The NRB Group since October 2015 and will be fully integrated with NRB S.A. by the 1st of January 2017.


e. info@nrb.be
t. +32 (0)4 249 72 11
f. +32 (0)4 248 11 70

**www.nrb.be**
@daringtocommIT
linkedin.com/company/nrb

NRB S.A. / nv
Parc Industriel des Hauts-Sarts
2e Avenue 65 | 4040 Herstal

Rue d'Arlon / Aarlenstraat 53
1040 Bruxelles / Brussel


NRB
DARING TO COMMIT