Industrialise your GDPR programme for faster, more assured compliance

Now that your GDPR programme is in place, how is it performing?

To what extent are compliance processes embedded in business-as-usual activities? How much administrative effort is involved in addressing topics such as data discovery and Subject Access Requests, and how well can your programme scale without distracting key personnel from core activities?

To address these questions and enable organisations to comply with the GDPR in a rapid, efficient and highly effective manner, Northdoor offers a range of solutions designed to industrialise compliance. Using technology-driven solutions, you can automate significant elements of your GDPR programme to gain greater assurance around compliance and ensure that your processes evolve over time.

northdoor
Store IT ◦ Protect IT ◦ Use IT ◦

A new beginning

For many organisations, the introduction of the General Data Protection Regulation (GDPR) in May 2018 represented the culmination of months or years of internal effort to create a fit-for-purpose compliance programme. While it may be tempting to draw a line under this effort, the GDPR's introduction should be seen more as a starting point than a conclusion. Now that the organisational structures are in place and the processes are defined, companies need to ensure that they execute their policies and best practices efficiently and effectively on a day-to-day basis. Recognising that both their organisations and the GDPR itself will continue to evolve, companies must continue to check for potential gaps in compliance and maintain internal assurance that their ongoing response to the legislation remains credible.

In plain English: you've implemented your GDPR programme; now what? Northdoor proposes the industrialisation of compliance processes, embedding them in business-as-usual practices such that they become a near-invisible, highly automated machine that enables internal personnel to focus on core business issues.

This paper outlines eight packaged solutions from Northdoor designed to address the key challenges that organisations face in managing their ongoing response to the GDPR. The solutions are designed to mesh together seamlessly, creating a comprehensive structure for assuring best practices with minimal organisational oversight. And for organisations that are still struggling to get their initial GDPR programme off the ground, all is not lost: Northdoor also continues to offer the GDPR Quickstart Assessment Workshop and related solutions to get you up to speed.

Northdoor solutions for GDPR industrialisation

- GDPR Programme Audit
- Data Discovery Solution
- Third-party Compliance Solution
- Subject Access Requests Solution
- Encryption Solution
- Data Masking Solution
- Data Protection Advisory Service
- Breach Reporting Solution

northdoor
Store IT • Protect IT • Use IT

GDPR Industrialisation Solutions

1 – GDPR Programme Audit

Accountability is a core principle of the GDPR: organisations must be able to demonstrate that they have analysed requirements in relation to their processing of personal data, and implemented a programme that enables them to achieve compliance.

Northdoor offers a comprehensive, structured review of existing GDPR programmes to confirm their fitness for purpose and ability to deliver credible compliance. Based on a series of workshops with key decision makers in your organisation, and guided by our proprietary methodologies and expertise, the Northdoor GDPR Programme Audit produces a clear report on potential shortcomings in your GDPR programme, with detailed step-by-step recommendations for remediation. The Audit is designed as a repeatable exercise, so that organisations can ensure their programme evolves in line with their own changing practices and with any modifications to the regulatory landscape.

Many organisations have made significant financial investments in achieving compliance with the GDPR ahead of the May 2018 deadline. The resulting programme should be seen as an asset to be serviced over time – if you treat it as a one-off investment in a static capability, you run the risk of exposing your organisation to compliance risks and having to perform a second full-scale implementation several years down the line. By running a Northdoor GDPR Programme Audit on a regular basis, you can ensure that your programme keeps pace with the changing world in an economical way.

2 – Data Discovery Solution

As the penalties for non-compliance with the GDPR are potentially severe, it is critical to understand where sensitive data is held and who has access to it. In the typical organisation, there may be anything from dozens to hundreds of systems that contain elements of personal data on customers, employees and business partners. These may include: data marts and warehouses, archival data, test/dev environments, outsourced mailing lists, and countless spreadsheets on laptops, NAS drives, USB keys and online file shares.

Your GDPR implementation doubtless included a data-discovery stage, but it is clear that systems, data and access rights are in constant flux. This means that data discovery must be embedded as an ongoing capability, taking advantage of automated tools to find, explore, analyse and classify both structured and unstructured forms of personal data.

The Northdoor Data Discovery Solution locates sensitive data stores and documents, highlights the relationships between structured databases, and reveals the access rights and security arrangements that govern them. It provides data maps and dashboards to increase organisational visibility of protected assets, and uses intelligent fuzzy searches to discover personal information hidden away in forgotten parts of your network.

By deploying a lightweight, web-based solution that provides best-practice ongoing data discovery across on-premises and cloud infrastructure, backed by Northdoor's expertise in defining search and classification policies, your organisation can maintain a clear view of the personal data you hold even as your business evolves and grows.

3 – Third-party Compliance Solution

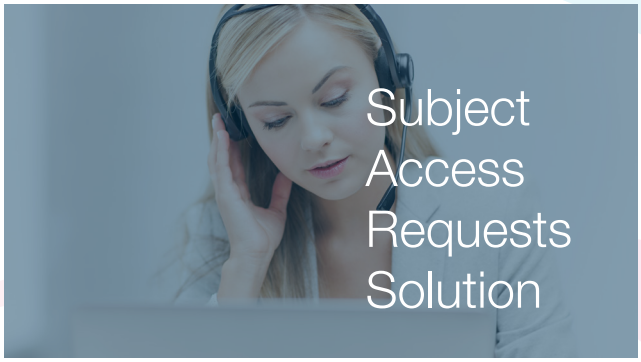
The GDPR obliges organisations to safeguard personal data, and extends responsibility beyond their four walls and out to partner organisations. If your company shares data with third parties – for example, for use in credit-risk scoring, market research or payroll activities – you retain joint responsibility for that data, and can be held jointly liable in the event of a breach.

Understanding data-protection risks is hard enough for internal systems. When external organisations come into the picture, each with their own partners, and their partners in turn, the resulting web of dependencies makes it even harder to understand exposure.

For many organisations, monitoring third-party compliance around the GDPR involves significant manual work in getting external partners to complete checklists. The time taken to gather and analyse the information typically makes this an annual exercise, potentially leaving you exposed to risk for months at a time.

To enable informed decisions and help your organisation operate securely in an open and collaborative digital world, the Northdoor Third-party Compliance Solution integrates third-party risk management into your enterprise risk management strategy.

Drawing on a comprehensive framework for identifying and managing digital risks, backed by machine-learning tools that can determine exposure across multiple degrees of relationships, the Northdoor solution automates compliance monitoring to provide an executive view of cyber risk in real time.



4 – Subject Access Requests Solution

Under the GDPR, data subjects (that is, natural persons) have more rights over the data you hold on them than ever before. These include the rights to see, edit, correct, export and erase any or all personal data – and organisations are required to make this a fast and easy process for the data subject.

Naturally, even a small number of Subject Access Requests (SARs) could represent a major distraction and drain on resources for an organisation, and a spike in requests could break manual processes altogether, leaving you exposed to the risk of regulatory action for failing to meet your SARs obligations.

Northdoor provides a complete Subject Access Requests Solution to increase both the accuracy and the speed of responding to incoming SARs. The solution offers a standardised framework for receiving requests through a convenient web portal, validating them, managing them centrally, automatically applying for extensions if there is a risk of exceeding the standard one-month deadline, and securely sending the requested information back to the applicant.

As part of the solution, Northdoor works with companies to automate their SARs workflows from assignment to approval, and to integrate with internal and external data sources for automated modification or erasure of data. The solution brings together all the requested information into a single, standard response to each data subject, ensuring consistency, precision and timeliness without tying up internal resources in manual paperchases.

5 – Encryption Solution

While the GDPR does not require personal data to be encrypted, many organisations rightly recognise that a properly implemented and managed corporate policy to encrypt data at rest and in transit can be extremely valuable.

Encryption is certainly not a silver bullet for compliance with the GDPR; for example, data will need to be decrypted for use, presenting the risk of improper access or dissemination by employees or partners. Nevertheless, encrypting your data can provide a vital second line of defence by ensuring that many types of breach will have no practical impact. And in terms of accountability, organisations may consider that any failure to take what is a relatively simple technical action might reflect badly on them in the event of a regulatory investigation.

Encrypting a single file or disk is easy even for non-technical users. Encrypting data of all kinds across hundreds of sources without impacting performance, and managing all the related keys and safeguards over time, is a major challenge.

Northdoor offers a comprehensive Encryption Solution that simplifies the creation and management of encryption policies across on-premises and cloud-based systems. Sensitive data can be automatically locked down, and access rights can be securely granted to employees and partners on an as-needed basis, with automatic revocation to keep data safe. The solution provides a single point of control for encryption, dramatically reducing the workload for IT personnel while improving the overall security posture.

6 – Data Masking Solution

Alongside encryption, the pseudonymisation or masking of data is a vital component in the enterprise IT toolbox. For requirements such as employee training or the development and testing of new software, organisations often need sets of “real” data. For example, testing a logistics app will require a list of customer names and addresses in standard formats, to ensure that the finished product works in the real world. Rather than using genuine customer data, which would present a risk under the GDPR, organisations typically use manual or automated masking techniques to create fictitious sets of data.

Creating masked data can be a major drain on time and resources, and existing manual processes may not be fully compliant with the GDPR. As time-to-market pressure grows, would your organisation benefit from the automated creation of realistic masked data?

Northdoor offers a fully automated Data Masking Solution that empowers organisations to take back control, improve the auditability of GDPR processes and save time for their IT personnel. The solution masks data accurately and in a context-aware manner to preserve integrity, and propagates masked elements consistently across applications to generate valid results in usage. In this way, the solution boosts internal efficiency, improves the effectiveness and demonstrability of compliance, and drives higher quality in testing and training data.

7 – Data Protection Advisory Service

Under the GDPR, all public bodies and any organisations whose core activity is conducting large-scale systematic monitoring or processing large amounts of sensitive personal data must appoint a Data Protection Officer (DPO). In the digital world, large amounts of activity do not necessarily imply large organisations, and many companies may struggle to find and retain a DPO with the right skills and expertise.

Employing a DPO may represent a challenge to core business activities, and there may not be enough work to justify a full-time, permanent position – raising the risk that candidates may seek more stimulating employment elsewhere.

The Northdoor Data Protection Advisory Service is designed to help you rapidly and cost-effectively access the expertise you need for addressing GDPR compliance. Via a simple annual subscription, Northdoor provides an expert Data Protection Advisor as required to serve as an independent data protection specialist. Your Advisor can assist with the implementation of privacy-by-design and data protection impact assessments, serve as the contact point for data protection authorities, and oversee data breach management and reporting.

By using the Northdoor Managed Service to engage a specialist with deep, ongoing experience of working in multiple different client environments, your organisation gets the benefits of world-class expertise at a fraction of the cost and without a long-term obligation to maintain additional headcount.

8 – Breach Reporting Solution

The GDPR mandates that organisations notify the relevant supervisory authority – in the UK, the ICO – of all data breaches "without undue delay" or within 72 hours, unless the breach is unlikely to present a risk to individuals. In scenarios where the organisations identify a high risk to individuals, there is also a requirement to inform everyone whose data was breached.

As part of your GDPR programme, you should have created a mechanism and organisational structures for identifying and responding to breaches. As with SARs, one of the key ongoing challenges is to be sure that your internal capability can work at scale and without incurring significant administrative overheads. If your organisation is dependent on nominated personnel to execute manual processes around breach reporting, there is a strong risk that you will be unable to meet your statutory obligations in the event of a major incident.

To help organisations cut the time required to identify and respond to breaches, Northdoor offers a comprehensive Breach Reporting Solution that ingests information from multiple systems (including SIEM and helpdesk systems) to provide a clear view at critical times. With embedded workflows and best practices, the solution guides employees through the reporting process and provides integrated security tools to help investigate incidents and prevent recurrence. The solution also maintains evidence of adherence to internal rules and best practices, and enables the simulation of incidents to test response plans and timelines. As external regulations evolve, the Northdoor solution keeps pace with changing standards in breach reporting, helping you remain compliant and avoid penalties

For more information

For organisations seeking assurance that their GDPR programme will continue to meet the ICO's compliance requirements without consuming internal focus and resources, Northdoor offers a comprehensive suite of solutions for industrialising processes and embedding them in the day-to-day fabric of the business. If you have invested heavily in getting the appropriate GDPR programme in place, and want to be certain that you're delivering effectively and efficiently, Northdoor can help.

Northdoor has decades of experience in providing compliant data-management solutions to hundreds of blue-chip businesses. With expertise and multiple external credentials in cyber security, including access-management controls, Northdoor has the skills to protect your business against data loss and exposure while supporting secure data sharing to drive growth.

For more information on how to move your GDPR programme into business-as-usual, contact Northdoor.


northdoor
Store IT • Protect IT • Use IT
DATA
GLOBAL MAP
JOHN
SAM
LISA