How does IBM support clients around data protection (GDPR) and cyber security (NIS) legislation?

In 2016, significant new cyber security and data protection legislation is being adopted in Europe: the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive. These legislation changes will affect customers in Europe, as well as those around the world doing business with Europe. IBM has been working on these issues for the last few years. In this paper, we share our perspective on some of the key changes, their implications and how IBM can help clients prepare for the changes necessary to meet the new regulatory and compliance requirements.

The new General Data Protection Regulation

Current European Union (EU) Data Protection rules date back to 1995. The EU was keen to establish a new set of rules that reflected the current reality of data usage and in response to calls that existing data protection laws were out of date. In January 2012, the European Commission made a proposal for a single harmonized General Data Protection Regulation across the EU.

After four years of intense negotiations, a political agreement on the General Data Protection Regulation was finally reached in December 2015. This was formally adopted into European law in May 2016[1]. Companies now have two years to implement and conform to the new regulation, which will enter into force in 2018. A parallel Directive affecting the processing of data by law enforcement authorities was agreed at the same time[2].

Member States and their relevant National Data Protection Authorities (DPAs) will now provide clarification and informative guidelines to help companies implement the regulation and to continue to do business with legal certainty. The National DPAs will build a European Data Protection Board that will coordinate the national DPA's across the EU and issue opinions on different aspects of the regulation to guide the implementation phase.

What are the implications?

The GDPR introduces significant changes to how companies must handle and process personal data. Processes from collection, processing, retention and deletion will have to be revised so they are compliant under the stricter data protection rules. Internal governance processes will have to change. For example, new data governance obligations will require companies who

[1] General Data Protection Regulation – Final Text
[2] Directive affecting the processing of personal data for law enforcement purposes

process data to prepare and keep records of processing activities, and also to demonstrate how decisions to use data for further processing have been reached. Even more than today, personal data must be processed in a transparent manner, collected for explicit and legitimate purposes ('purpose limitation'), limited to what is necessary in relation to the purposes for which they are processed ('data minimization') and must be accurate (and kept up to date).

New rights for Data Subjects

Data subjects, people whose personal data is stored, have new mandatory rights which give them more control over their personal data. This includes, amongst others, the right to be forgotten (erasure) and the right to data portability. Data subjects who require more information on their data and the rights they have will also be able to request that more easily than they can today, and information about actions taken to satisfy their rights need to be provided within a month in principle.

- Consent must be clearly distinguishable from other written declarations and cannot be hidden within other information notices.
- Privacy policies surrounding data processing on these aspects will be longer and more detailed.
- Companies will have to keep a track record to show where the different sources of data have come from, how the data has been collected, and demonstrate the explicit consent of the data subjects.

There will thus be an increase in administrative burden in these areas and will be particularly difficult for companies who still store data on paper.

New responsibilities for Data Controllers & Data Processors

The regulation introduces a new concept of joint liability for both data controllers and processers under which data processors are now jointly liable to data subjects for damages unless they can prove that a breach, for example, was not their fault. This now also means that previous contractual obligations may need to be revised, and new contracts will require appropriate stipulations.

Data controllers will have more responsibility to provide concise information on how data is processed. For example, they will have to detail the retention period of storage of the data and need to inform about the legal basis for the processing. In addition not only data controllers, but also data processors need to maintain records of their processing activities.

The principle of 'Data Protection by Design' is emphasized in the new regulation, and needs to become part of best practices in all product life-cycles. Each part of designing or compiling a

new solution needs to show that the rights of the data subject were taken into account. This can for example be used through methods of pseudonymization or encryption.

The regulation also introduces a new security breach notification, which is applicable for all data controllers across sectors. Data processors have to report respective breaches to the data controller. Data controllers must now also report security breaches to their supervisory authority without undue delay and, where feasible, no more than 72 hours after having become aware of it. In some cases, individuals need to be notified directly.

Privacy Impact Assessments will be required when organizations want to undertake certain type of processing of personal data.

Transfer of Personal Data (Data transmission to Third Parties)

The transfer of personal data provisions remain largely the same as was outlined in the previous directive. Transfer mechanisms such as Model Clauses and Binding Corporate Rules can still be used. Data transfers under the mechanisms of 'Safe Harbor' are no longer permissible, following its invalidation in October 2015. For data transfers previously held under 'Safe Harbor,' the renamed 'Privacy Shield' agreement has yet to be approved by the EU Member States. This transfer mechanism has more stringent rules then the previous Safe Harbor agreement. For example, it offers more channels for the data subject to seek redress.

How can IBM help?

IBM offers services and solutions which can help clients around the world prepare for these changes. Some examples include:

- **IBM Data Privacy Consulting Services** can help customers identify areas of their business which may be impacted by the GDPR. IBM Consulting experts work with clients to help them on organization design, and developing and implementing solutions in line with data privacy requirements, as well as from an operational, information technology and information security perspective, all of which are key to data privacy/protection compliance.
- **IBM Security Solutions** help detect, address and prevent security breaches, through integrated hardware and software solutions. IBM® Security Guardium is a comprehensive data security platform that provides a full range of capabilities – from discovery and classification of sensitive data to vulnerability assessment to data and file activity monitoring to masking, encryption, blocking, alerting and quarantining to protect sensitive data.

- **IBM Cloud & Cognitive Services** are transparent and agile enough to fit our client's needs. In general, clients will need help ensuring they are compliant in the way they process personal data through their internal (governance) processes, by keeping track of and reporting data breaches, and documenting how data is obtained, from where, on what date, etc.
- **IBM Information Integration & Governance (IIG)** can provide agile data integration and governance to build confidence in data exploration and management. The IIG also can provide insight into unstructured data, and also the tools and methodologies to instrument and enforce policies.

The new Network and Information Security Directive

In 2012, the commission proposed a new law to drive enhanced cyber security across Europe, stating that existing capabilities were not sufficient to ensure a high level of security of network and information systems within the Union. The Network and Information Security (NIS) Directive is the resulting new legal framework in Europe covering cyber security or Network and Information Security. It is going through its final processes to become law in 2016. This new EU law directs Member States to create or adapt their laws covering Network and Information Security in line with the scope of the directive.

European Member States will have 21 months to implement the NIS directive – each national government will use the directive as their "template" to adjust local laws. This process starts once the directive has been finalized and published and will continue through 2018, until the maximum amount of time each Member State has to implement the directive has expired. Some Member States have already started to align their national cyber security strategy, their operational capabilities and their legislation with the directive.

In the new legislation, operators of essential services in critical industry sectors are placed at the highest risk level, and areas such as cloud computing providers are subject to a lighter touch approach in a new category of providers called digital service providers (or DSPs).

What are the implications?

The NIS Directive imposes a new set of security obligations and incident reporting requirements on a broad set of private sector companies, many of whom are IBM clients. The primary focus will be on operators of essential services in critical industry sectors, as well as on incident reporting requirements for a broad set of DSPs – online search engines, online marketplaces and cloud computing providers. The directive however goes further into requiring appropriate security measures. Some of the core changes which are being driven in the directive are:

New requirements for Incident Reporting

Thresholds are now set out to determine whether an incident should be categorized as having a significant impact on the continuity of essential services, and would thus need to be notified by operators of essential services to the relevant government authority. The aspects which will need to be particularly considered now include:

- Number of users affected by the disruption of the essential service;
- Duration of the incident;
- The geographical area affected.

New Government National Regulatory Authorities

Organizations will see new arrangements being put in place for coordinating cyber security issues. Each Member State government will set out one or more competent national authorities responsible for fulfilling the tasks linked to the security of the network and information systems of operators of essential services and DSPs. These governments also will be required to designate in each country a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross–border cooperation at the EU-level.

New National Cyber Security Capabilities

Organizations will also see Member State governments directed to ensure that every EU Member State has in place well-functioning Cyber Security Incident Response Teams (CSIRTs), also known as Computer Emergency Response Teams (CERTs). These will have to meet essential capability requirements for dealing with incidents and risks, and ensuring efficient cooperation at the Union level.

New Risk Management requirements

The NIS directive calls for a culture of risk management, involving risk assessment and the implementation of security measures appropriate and proportionate to the risks faced. These are to be promoted and developed through appropriate regulatory requirements and voluntary industry practices. This will potentially require IBM clients to demonstrate that they are conducting risk assessments, and that they have implemented appropriate security measures. Some requirements already exist around risk assessment and reporting with respect to essential services, and new requirements for essential services may be set at national level. Operators of essential services under this legislation include operators in the following industry sectors: energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructures such as internet exchange points. The other category of DSPs will see requirements created on a pan-European basis.

How can IBM help?

As the NIS Directive is being rolled out across Europe, clients are asking for our views, for help in understanding how the directive can be applied, and whether we have services and solutions available to bolster their Network and Information Security. Examples of relevant IBM offerings include:

- **IBM Security Consulting Services** are helping clients build Security Operations Centers and Computer Emergency Response Team (CERT) capabilities. We are helping clients optimize existing capabilities, and develop a strategy and plan to build next-generation threat intelligence, enterprise monitoring and security operation centers.
- **IBM X-Force Incident Response Solutions** are helping clients plan for and manage security incidents. Consulting teams are working with clients to create security incident processes and, with the new capabilities of IBM Resilient Systems solutions, helping clients collect and manage information in connection with their compliance requirements.

These are examples of the range of capabilities - from risk assessment, developing and implementing appropriate security measures and enabling capacity around incident reporting – available to clients looking to run their own operations, or reaching out for cloud and managed service delivery models.

Summary

The evolving European regulatory environment on cyber security and data protection offers both possibilities and challenges for both IBM and our clients. These challenges range from governance to securing application and infrastructure. Fundamentally, it is important to assure stakeholders of IBM's expertise and capabilities in these areas in order to build upon existing trust and confidence in our brand.

IBM has extensive experience helping clients navigate regulatory environments in Europe and around the world. We have done this successfully through consulting services and solutions and through our delivery of cloud and cognitive solutions. This paper reflects IBM's general view of Europe's new regulatory landscape. It is not, however, intended to be exhaustive and does not describe every procedure and technical detail that could be required.

The key to establishing preparedness in this new era lies in choosing the right partner(s) for your organization, and being able to deploy appropriate security and data protection controls and procedures in a way that can be rapidly and readily demonstrated. We understand this is not just a technical challenge, but a challenge of governance and compliance, applications and infrastructure and assurance.

Author Nick Coleman
IBM Global Head Cyber Intelligence
Email: coleman@uk.ibm.com
twitter.com/colemansec