Preview

Guidelines for Outsourcing, Offshoring, and Cloud Services

Foreword

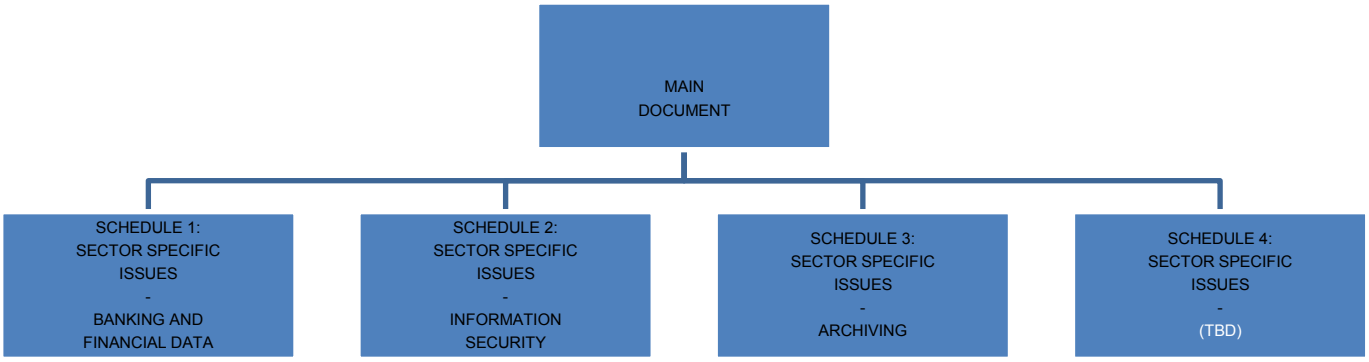
Data security and data protection challenges arise in most outsourcing and offshoring transactions, particularly where services are cloud based. Unfortunately, these challenges are often resolved at the last minute, resulting in higher costs, unwieldy solutions and the increased prospect of regulatory intervention.

In many cases, data governance issues are not addressed early enough because the parties do not know where to begin the dialogue or how to identify relevant concerns. There is little practical guidance in the market which addresses both data security and data protection issues in the context of international outsourcing and offshoring transactions. The advent of the provision of cloud-based services is bringing these issues into sharp focus.

The document is a result of the cooperation between ICT Norway and Intellect (a UK technology industry trade association), with the contribution from several representatives from both private and public sector. Deserving special mention in this respect are the following players: Accenture AS, Evry AS, the Financial Supervisory Authority of Norway, Itera ASA, Logica Norge AS, Microsoft Norge AS, the National Archives of Norway, NorSIS and Sparebank1. Our main intention with this document is merely to provide parties with relevant and practical guidelines describing the steps that could or need to be taken in order to increase the level of compliance and to reduce the level of unwanted exposure. It is important to note that information provided in these guidelines is not intended nor recommended as a substitute for professional, legal or other advice.

We have deliberately focused on data privacy matters in the context of outsourcing and offshoring transactions, as this is highly relevant for many parties involved. However, it is important to note that different kinds of transactions in most cases will also give rise to other legal matters in addition to data privacy matters in cross-border situations. Therefore we provide a section with a legal overview of the sector specific regulations that may be of relevance depending on the characteristics of the transaction (cf. Section 4 - Legislation overview (Norway)).

The overview may be expanded with a more in-depth analysis upon request and/or in a later edition of these guidelines. If so happens, the analysis and specific guidelines regarding sector specific regulations may be added as schedules to this main document. Accordingly, an example of the structure of the document would be as shown in the figure below:



We feel that wider debate of these matters, from both a security and a data protection perspective and for all the phases in the outsourcing lifecycle, will ensure that these issues are dealt with pragmatically and constructively in the future; particularly as cloud computing achieves wider prominence. Hopefully, these guidelines will encourage parties to discuss these complex challenges as early as possible in the outsourcing lifecycle.

Contents

1. Introduction to the guidelines

What are the guidelines?

Data security and data protection requirements frequently trigger friction and frustration in international outsourcing and offshoring transactions. Too often, this is because the parties do not understand their respective obligations or are unable to identify and focus on the key issues.

This set of guidelines will encourage vendors and customers to work together to anticipate and address the data security and data protection issues which may affect the success of their outsourcing projects.

The guidelines also seek to eliminate last minute frustrations by providing both customer and vendor with a clear overview of the types of issues which arise, the stage of the project at which they can most easily be addressed, and indicating which party is best placed (or legally obliged) to deal with the issues.

Key definitions and explanations

For ease of reference we include below some definitions and explanations of a limited selection of the most important terms that are being used in these guidelines. For further clarification of terms and phrases being used throughout this document, please see the Glossary in Appendix D and also Appendix B for explanations of the most common terms related to data privacy.

- Outsourcing: Most commonly the term “outsourcing” refers to the transmission of services, production, processes or activities to an external provider. The term is often used together with a description of what services, processes etc. that are being outsourced. For example, so-called “business process outsourcing” typically includes transmission of HR functions and associated operational activities to a third party. Among many other examples are “IT infrastructure outsourcing” and “IT application management outsourcing”.

- Offshoring: “Offshoring” as referred to in this document means the relocation of services, production, processes or activities from one country to another. As for the relationship to the term “outsourcing” as explained above; when the “offshored” services, processes etc. are being transferred to an external provider in that other country, the situation may be described as “offshore outsourcing” (as opposed to “onshore outsourcing” where the outsourcing is performed within one country). It may be the case that the other country is not “offshore” in the strictest sense of the word, for example the other country may be a nearby country, often sharing a border, where both parties expect to benefit from one or more of the following dimensions of proximity: geographic, temporal (time zone), cultural, linguistic, economic, political, or historical linkages. In these cases the term “nearshoring” may be used.

- Cloud: According to the official National Institute of Standards and Technology's (NIST) definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The terms “Cloud”, “Cloud computing” and “Cloud services” are in this document interchangeable terms unless otherwise specified or obvious considering the context.Examples of service models for “Cloud computing”:

    - “Software as a Service” (“SaaS”), which is a model of software deployment over a network where the customer uses the provider’s application(s) on a cloud infrastructure;
    - “Platform as a Service” where the customer deploys customer-created/-acquired applications onto the provider’s cloud infrastructure using programming languages and tools supported by the provider; and
    - “Infrastructure as a Service” (“IaaS”) which refers to the delivery of computer infrastructure as a service over a network.

  “Cloud” is related to “offshoring” in the sense that the external provider and its servers may be situated in another country than the user. Also, “Cloud” is related to “outsourcing” in the sense that the delivery of “cloud”-services may be a way of the Customer to “outsource” some of its services, production, processes or activities to an external provider.

- Personal data: Data that relates to a living individual who can be identified from those data, or from those data and other data in the possession of the data controller (cfr. below).

- Data controller: Person/company who determines how and for which purposes personal data is to be processed. Often the Customer is the original data controller who wishes to "outsource" the processing (and occasionally) control functions to a third party vendor. The processor may be situated in another country ("offshore"). Please note that the categorization of "data controller" and "data processor" (cfr. below) may be difficult, and that there are substantially different legal requirements applicable depending on whether the party is a "data controller" or a "data processor".

- Data processor: Any person/company, other than an employee of the data controller (or that the data controller has the power to instruct), who utilises or processes personal data on behalf of the data controller, for example as part of an "outsourcing" agreement. The processor may be situated in another country ("offshore"). Please note that the categorization of "data controller" (cfr. above) and "data processor" may be difficult, and that there are substantially different legal requirements applicable depending on whether the party is a "data controller" or a "data processor".

Why are the guidelines important?

In recent years, the media has been inundated with stories relating to data breaches in both the public and private sectors. In response to the public's concerns about the security of their data, EU regulators have become more proactive in raising awareness of individual's rights and enforcing compliance. In turn organisations are becoming increasingly more focused on addressing data security and data protection issues, recognising that data is often an organisation's most valuable asset.

Failure to comply with the data security and data protection regulatory framework may:

- expose an organisation to financial risk (eg. delayed implementation and/or the costs of remedying a breach);
- result in damage to an organisation's reputation - the regulators are quick to publicise data breaches in the press which may compromise trust in an organisation;
- result in enforcement action (eg. an organisation may be prevented from processing data, or be required to implement compliant practices);
- expose an organisation to civil penalties (eg. fines by regulators);
- result in an organisation's officers and directors being convicted of a criminal offence.

Most outsourcing projects require data to be transferred from customer to vendor, frequently on an international basis. Data security and data protection laws affect how data may be transferred between the parties. Increases in global data use and technological developments have made data security and data protection challenging. An additional level of complexity arises where the data are transferred between multiple jurisdictions, particularly where the vendor utilises a cloud-based infrastructure.

Many of the obligations rest with the customer, as owner of the data; however, in an outsourcing context, customers (unlike vendors) do not usually deal with data issues. This can result in misunderstanding of data security and data protection requirements. It is essential that data security and data protection considerations are included in the initial vendor due diligence. Both the customer and the vendor should carefully analyse the proposed solution to ensure regulatory compliance issues are addressed. Crucially, if identified early in the outsourcing process, data issues can be dealt with in a practical, compliant and efficient manner. If ignored during the early stages of an outsourcing project, data issues can delay implementation or even require fundamental re-thinking of the structure of the data processing activity.

How do the guidelines work?

These guidelines offer a checklist of common data security and data protection issues, structured around an outsourcing transaction and addressing offshore and cloud aspects where applicable.

The guidelines identify issues that typically arise at each of the stages of the outsourcing lifecycle and indicate which party (customer or vendor) is usually responsible for dealing with the issues.

The early visibility of issues determines the expectations of both customer and vendor, enabling both parties to anticipate and begin to address data issues from the outset of the project. This lead-time can be critical to developing efficient and cost-effective solutions to issues.

Who should use the guidelines?

This set of guidelines is intended for customers who, typically, do not deal as often as vendors with the data security and data protection issues that arise in an outsourcing context.

The guidelines will also be a useful tool for vendors. They provide a resource for enabling the parties to work collaboratively to address at an early stage issues which, if ignored, can cause unnecessary and unforeseen costs and delays later in the project.

The guidelines will be relevant for parties working in both public and private sector.

Increases in global data use and technological developments have made data security and data protection more challenging. An additional level of complexity arises where the data are transferred between multiple jurisdictions, such as when a vendor utilises a cloud-based infrastructure.

For what types of projects should the guidelines be consulted?

The guidelines should be consulted for all outsourcing projects which involve data processing.

They will be particularly useful where personal data relating to individuals are processed. European data protection laws require careful consideration of data security and data protection issues in an outsourcing context, especially where personal data are transferred outside the EU, or into the cloud.

Several non-European jurisdictions also have either comprehensive or sectoral data protection laws and regulations, such as India, Ukraine, China, Russia and the United States of America. Resources relating to the data protection laws in key outsourcing jurisdictions are set out in Appendix B. In addition, Appendix C provides an overview of emerging EU data breach laws.