UPDATE and RECAP GDPR (Global Data Protection Regulations)

The European Union data protection law requires organizations to take adequate measures to ensure the security of personal data. This obligation must be met regardless of the means used to process the personal data. The security obligation covers not only enterprise information systems, but also cloud services used to process the personal data. Data breach notification obligations, steep fines of 20 million euro or 4% of global turnover, whichever is higher, and increased public scrutiny of how organizations use and protect personal data require that they pay close attention to the security of personal data.

One of the central principles of the European Union's new General Data Protection Regulation (GDPR or regulation) is its Accountability Principle: organizations must demonstrate that they comply with the GDPR and that they have taken appropriate measures to ensure compliance. Add the new 'right to be forgotten' and the new privacy principles of Data Protection by Design[1] and Data Protection by Default[2] and one can conclude that managing compliance with the GDPR is going to be a challenge.

The compliance problem of unmanaged cloud services

One of the most underestimated compliance challenges that organizations face under the GDPR is the fact that many - if not most - personal data for which the organization is legally responsible are processed in an unstructured way. They are not processed in pre-de need enterprise data systems or pre-approved cloud services that comply with the organization's security policies and legal obligations, that meet the data minimization and data quality principle, and that are regularly backed-up, patched and audited as part of the organization's management cycle. Also, unstructured personal data are created by users – often unsupervised – using productivity or collaboration applications. These data are stored on mobile devices and shared with others through unsanctioned applications and cloud storage locations, which are outside the organization's direct control. The trend of Bring Your Own Device (BYOD) has only exacerbated this problem.

Nevertheless, under the GDPR it is always the organization's legal responsibility to protect such unstructured data from loss, alteration or unauthorized processing, even if workers use cloud services that are not pre-approved or controlled (sanctioned) by the organization. This means that organizations must:

Know which personal data are processed by users of cloud services;

Identify the cloud applications used by the organization's workforce;

Prevent personal data from being stored or processed in unmanaged cloud services; and

Protect personal data when stored or processed in cloud services. Failure to manage non-approved cloud services may leave the organization at serious risk, from both a legal perspective and from a business continuity and reputational perspective. CIOs should therefore pay close attention to this issue and implemer measures to bring such cloud services under the visibility and control of the organization.

The GDPR in relation to cloud services

The rules of the GDPR apply regardless of the means used to process the personal data. They apply to personal data stored on local servers, as well as on servers in the cloud. However, the cloud poses a number of specific compliance challenges to entities covered by the GDPR:

The GDPR requires that controllers and processors **know the location** where the personal data are stored or otherwise processed. The GDPR severely limits the ability of entities covered by the GDPR to transfer the personal data to recipients outside the European Economic Area (EEA, as in the Member States of the EU, plus Norway, Iceland and Liechtenstein). Cloud services may use servers outside the EEA unknown to the controller or processor, or the cloud service's data processing equipment in European territory may be remotely serviced by non-EU service providers. In all such cases the transfer of personal data must comply with the data transfer rules of the GDPR.
The GDPR requires that controllers **take adequate security measures** to protect the personal data from loss, alteration or unauthorized processing. The controller should **assess** whether the security measures of the processor meet the security requirements applicable to the personal data (on the basis of a risk analysis) and to the controller (on the basis of specific sectoral, contractual or organizational requirements) and must supervise the implementation of security measures by the processor by conducting regular audits. The same obligations apply to the processor using a sub-processor. However, most cloud providers do not allow their clients to provide instructions relating to data security or to conduct security audits.

The GDPR requires the controller to **close a 'data processing agreement'** with the processor. Such a contract must stipulate a number of particular obligations on the part of the processor, such as:

- to act only on the instructions of the controller;

- to take adequate security measures to protect the data from loss, alteration or unauthorized processing;

- to engage a sub-processor only with the prior permission of the controller;

- to assist the controller if necessary in response to requests for exercising data subjects' rights;

- to assist the controller in meeting his obligation of notifying the supervisory authority and the data subjects of a data breach;

- to assist the controller in conducting a 'data protection impact assessment' to identify the privacy and security risks of the processing of the personal data; and

- to hand over all personal data after the end of the processing or the termination of the service agreement. However, most cloud providers provide their services on the basis of terms and conditions which do not meet these requirements and which are not or are only marginally negotiable.

The GDPR requires that personal data are **collected only as necessary to the purpose, puts limits on the processing of special data** (such as data revealing race, ethnic origin, biometrics, political conviction, religious or philosophical beliefs, data concerning health and sex life, union membership, and data relating to criminal convictions or offences) and **puts limits on the processing of certain sensitive data**, such as tax numbers and data relating to children. This requires a detailed assessment of the functionality and data elements of applications before they are put to use. Many cloud services only unveil their full functionality and data requirements after organizations have started to use them.

The GDPR does **not allow data processors to use the personal data for other purposes** beyond providing the services to their customers. However, many cloud services reserve the right to use the data for all kinds of secondary purposes, such as marketing. Especially when cloud services are offered for free, cloud providers use the data in some way to generate revenues. Some cloud providers even claim full ownership of the data stored in their environment and sell the data to third parties.

The GDPR requires personal data to be **erased when the purposes of use have ceased to exist.** This means that organizations must specify data retention limits for the data (in advance), have the data automatically erased from their systems or organize for the data user to take an informed decision on the further retention of the data, and conduct audits to check whether the data have actually been erased. Many cloud services are not clear about their data erasure procedures or tell their users to erase data, so the organization may be in breach of the regulation because the data are not properly erased from the cloud services.

Usefull links :

Final EU proposal on the protection of Individuals.
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT

OECD Guideline for Multinational Enterprices
http://www.oecd.org/corporate/mne/oecdguidelinesformultinationalenterprises.htm

Reform of EU data protection rules
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

EU Data protection Reform news
http://europa.eu/rapid/press-release_IP-15-6321_en.htm

European data protection for the digital era

Better protection for personal data

- Clear consent required to process data
- More and clearer information about processing
- Right to move data from one service provider to another
- Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'
- Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child
- Easier access to personal data
- Right to notification if data is compromised
- Stricter safeguards for transfers of personal data outside the EU

More opportunities for business

- Level playing field for all EU and non-EU businesses offering goods and services to persons in the EU
- One set of rules for the whole EU
- Rules that allow businesses, especially SMEs, to get the most out of the Digital Single Market
- Risk-based approach, matching obligations of controllers to the level of risk of the processing

More consistent application and effective enforcement

- Individuals and businesses can have their cases dealt with by a data protection authority and a court close to them
- A one-stop shop for individuals and businesses in cross-border cases thanks to the cooperation of national data protection authorities

Fines up to €20 million **OR** 4% of global annual turnover

Council of the European Union
General Secretariat