sia partners

INSIGHT

NOVEMBER 2017

ARE YOU ON THE RIGHT PATH TOWARDS GDPR COMPLIANCY?

Doomsday or scarecrow? Articles on the General Data Protection Regulation (GDPR) are published on a daily basis. Consultancy firms, lawyers and other experts frequently weigh in to explain the details of GDPR. Many publications raise the alarm, since no organization seems truly GDPR compliant. Consequently, fines (up to a maximum of 4% of annual worldwide turnover) and reputational damage could be enormous. Others perceive GDPR as just a paper tiger and state that many 'experts' are scaremongering to their own benefit.

We will not participate in the speculations – is GDPR doomsday or a paper tiger? - or hypothesize in what capacity the supervising authorities will enforce GDPR. Instead, we believe that the GDPR debate should be revolving around key questions such as 'how to manage GDPR compliance in your own organization' and 'what are best practices in implementing GDPR compliance?' To this end, we would like to share our experiences in guiding financial institutions in the Benelux towards GDPR compliance.

Introduction

GDPR compliance projects can be started in many. In our experience, it is advisable to begin the journey with holding strategic discussions with the GDPR sponsors in the organization. Its output will often be revealing, including at least:

1. the understanding of the client environment
2. the stakeholders
3. the scope (which business units or departments are in scope?)
4. the compliance ambition level, also formulated as the desired level of compliance

Why is the latter of such paramount importance? We understand that not all financial institutions aim for an A+ compliance mark. If your risk appetite is higher and your budget limited, aiming for a B- (approaching minimal viable compliance) could be a preferable outcome. Knowing your compliance ambition level at the very start of the project helps you defining priorities at a later stage.

To Be Design

Once we have a good overview of the deciding factors as described in the previous paragraph, we start with describing the To Be situation. The design on the To Be situation is dependent on the compliance ambition level of the organization. The legal department is a key stakeholder in the To Be design. Legal is pivotal in understanding the consequences of GDPR for the organization as well as aligning existing internal regulations or certifications. An important output of the To Be Design is a description of GDPR items. Think of at least the following items:

1. data protection principles;
2. lawful basis for processing;
3. consent;
4. rights of the data subjects;
5. obligations for controllers.

Once described, the GDPR items need clarification and 'meaning' to the organization. Let us have the item of 'rights of the data subjects' as an example. One of its components is the 'right to data portability', which means that individuals are entitled to transfer their data to another data controller. Consequently, the 'right to data portability' can be described as a sub item, linked to the main item. After the identification and description of each GDPR (sub) item, a large number of GDPR requirements will be drafted, which will be used in the next stage of the As Is design.

As Is Design

After completing the To Be situation, the As Is situation will be described. The As Is design will show which GDPR requirements have been already met and to what extent. Risk, Operations and Compliance departments can take a leading role in the 'scoring' of the GDPR requirements. If we return to our example of the 'right to data portability', the following questions could be asked among others to define the score:

1. Can we provide individuals with a copy of their personal data?
2. Which kind of data can we provide to individuals (specify data clusters; specify

data provided by the individual or data accessed via other sources)?
3. Is the format of providing data machine readable?
4. What are the existing timelines for providing data?
5. Which department and/or internal role is currently responsible for providing the data?
6. What are the dependencies for providing the data?
7. Has the data portability process been described and distributed to stakeholders?

These kind of questions help to bring objectivity to the scoring process and provide clarity in the GDPR compliance readiness of the organization.

In order to answer these kind of questions in an orderly fashion, it is essential to establish a complete overview of all personal data stored throughout the organization. Hence, it is necessary to record:

1. what kind of personal data (data clusters) has been stored;
2. in which files and systems these data has been stored (electronically and paper-printed);
3. the source(s) of the data;
4. the purpose of the data (from a client perspective);
5. who has access to the data (intra-organization, inter-organization, external, outside EU, etc.);
6. the current precautions in protecting the personal data.

Setting up a data inventory is a fruitful exercise, since the organization will be forced to consider the existing handling of personal data. The creation of several data inventories helped us understand that oftentimes certain types of data is stored in many different unaccounted places. Simultaneously, the gathering and keeping of these types of data rarely serves any client purpose. Furthermore, we commonly see that access to certain types of data has not been managed properly. As a consequence, many employees can access data, including sensitive data, while they are not authorized to do so. These actions conclude the To Be Design, after which the Gap Analysis will be conducted.

Gap Analysis

The Gap Analysis bridges the prior As Is and To Be Design. Let us continue with the example of 'data portability'. We assume that the As Is Design showed that the organization cannot provide a machine readable copy within the required timeframe. Consequently, the organization has 2 choices:

1. solving the issue
2. accept the non-compliance status

In case of the latter, the reasoning behind choosing this option has to be described. In case of the former, a prioritization will be assigned to solving the issue.
Accepting the non-compliance status of a GDPR item depends on three factors:

1. the probability that a GDPR item will occur
2. the practical implication of an occurring GDPR item
3. the compliance ambition level (desired level of compliance)

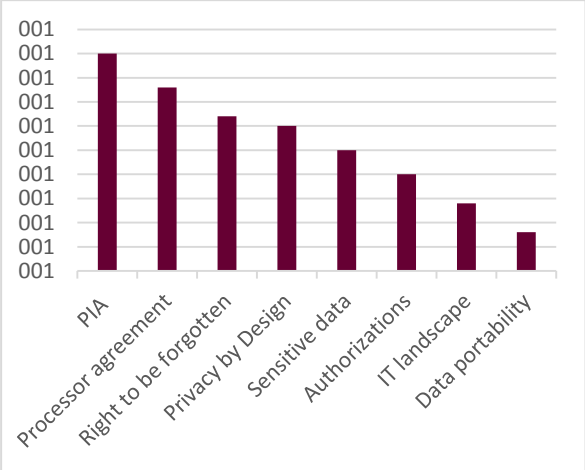
The non-compliance status of a GDPR item could be accepted by a financial institution, when the item has a low probability of occurring and when the item has limited practical implications. In our example: the possibility that a data subject will exercise his right of data portability is small, when a company has a limited amount of personal data of the data subject and when the data subject is a representative of a company (B2B client). The practical implications are limited because the data portability request, when the company has a limited amount of personal data, can be fulfilled in time on an ad hoc basis. For an explanation on the compliance ambition level, see the Introduction of this article.

Once all issues have been identified and prioritized, it is recommended to continue with the high priority issues. For each issue, solutions to these issues will be drafted. Each solution contains tasks. Tasks for the medium and low priority issues will be outlined at a later stage. The tasks include an approximate effort, approximate costs, action owners, dependencies, deadlines and whatever information the organization needs to complete the tasks. Once all items and sub items have been classified, prioritized and tasked

accordingly, the documented outcome is the basis for the Project Plan, which will be used in the next step: the implementation phase.

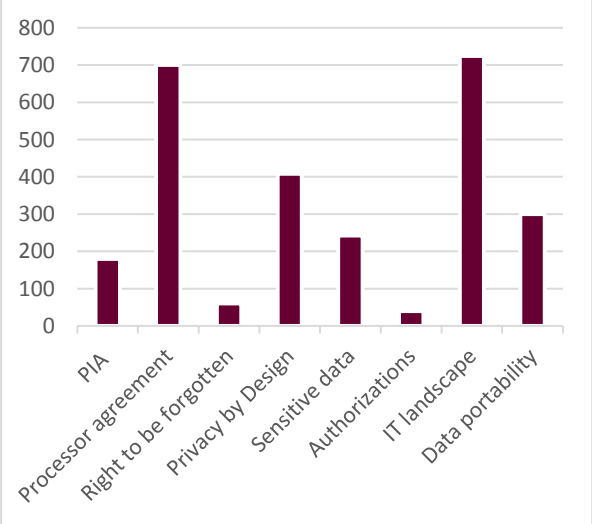
We show an element of a high level sample Gap Analysis below.

RISK IMPACT SCORE - EXAMPLE



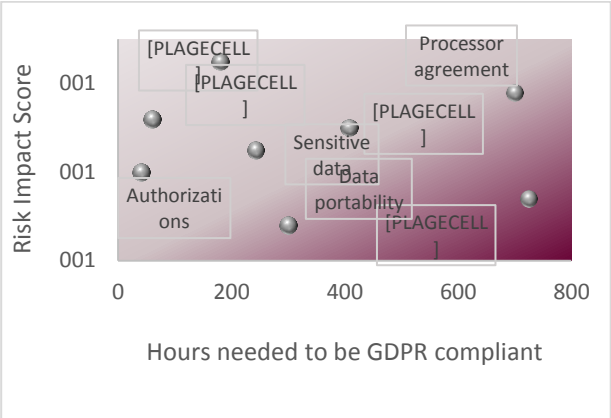
The Risk Impact Score is a result from the conducted analysis. The higher the score, the higher the non-compliance of the organization

HOURS NEEDED TO BE GDPR COMPLIANT - EXAMPLE



Another outcome of the analysis is the total hours needed for an organization or department in order to be fully compliant.

GDPR QUADRANT OF PRIORITIES - EXAMPLE



The outcomes of the two previous analyses are combined and plotted in the GDPR quadrant. It would generally be recommended to start with the items in the top-left corner: these are the quick wins.

The proof in the pudding

The implementation phase may be most difficult of all. Why? In this phase, many more departments (IT, Finance, HR, Marketing, Sales etc.) will play an important role. Sometimes, these departments may be either biased against compliance projects, too busy for the assigned GDPR compliance tasks or understaffed altogether. The dependency on a number of departments could make the implementation phase highly challenging. Furthermore, implementing GDPR compliance will frequently trigger a major change in these departments. These changes can be of technical, organizational and/or strategic nature. For example, think of the major consequences embedding 'Privacy by Design' in the DNA of each department.

In our next article, we will describe how we handled the implementation phase for one of our large financial clients in the Benelux. For now, we want to thank you for your attention. We strongly advise you to take a close look around: how has GDPR compliance been managed so far in your organization?

YOUR CONTACTS

STEPHAN LINNENBANK

Head of Financial Services Netherlands & Belgium
+31 (0)6 235 982 23
stephan.linnenbank@sia-partners.com

PAUL GEERTS

Head of Banking The Netherlands
+31 (0)6 5253 2665
paul.geerts@sia-partners.com

ABOUT SIA PARTNERS

Founded in 1999, Sia Partners is an independent global management consulting firm with over 600 consultants and an annual turnover of USD 120 million. The Group has 16 offices in 13 countries, including the U.S., its second biggest market. Sia Partners is renowned for its sharp expertise in the Energy, Banking, Insurance, Telecoms and Transportation sectors.

For more information visit : www.sia-partners.com . Follow us on Twitter @SiaPartners

Asia

Hong Kong
701, 77 Wing Lok St,
Sheung Wan, HK
T.+852 3975 5611

Singapore
3 Pickering street
#02-38
048660 Singapore
T.+ 65 6635 3433

Tokyo
Level 20 Marunouchi
Trust Tower-Main
1-8-3 Marunouchi,
Chiyoda-ku
Tokyo 100-0005
Japan

Europe

Amsterdam
Barbara Strozzilaan
101
1083 HN Amsterdam
- Netherlands
T. +31 20 240 22 05

Brussels
Av Henri Jasparlaan,
128
1060 Brussels -
Belgium
+32 2 213 82 85

London
Princess House,
4th Floor, 27 Bush
Lane,
London, EC4R 0AA –
United Kingdom
T. +44 20 7933 9333

Lyon
Tour Oxygène,
10-12 bd Vivier
Merle
69003 Lyon - France

Milan
Via Medici 15
20123 Milano - Italy
T. +39 02 89 09 39
45

Paris
18 bd Montmartre
75009 Paris - France
T.+33 1 42 77 76 17

Rome
Via Quattro Fontane
116
00184 Roma - Italy
T. +39 06 48 28 506

Middle East & Africa

Dubai, Riyadh, Abu Dhabi
PO Box 502665
Shatha Tower office
2115
Dubai Media City
Dubai, U.A.E.
T. +971 4 443 1613

Casablanca
14, avenue Mers
Sultan
20500 Casablanca -
Morocco
T. +212 522 49 24 80

North America

New York
115 Broadway 12th
Floor
New York, NY10006 -
USA
T. +1 646 496 0160

Montréal
600 de Maisonneuve
Boulevard West,
Suite 2200
Montreal, QC H3A
3J2 - Canada