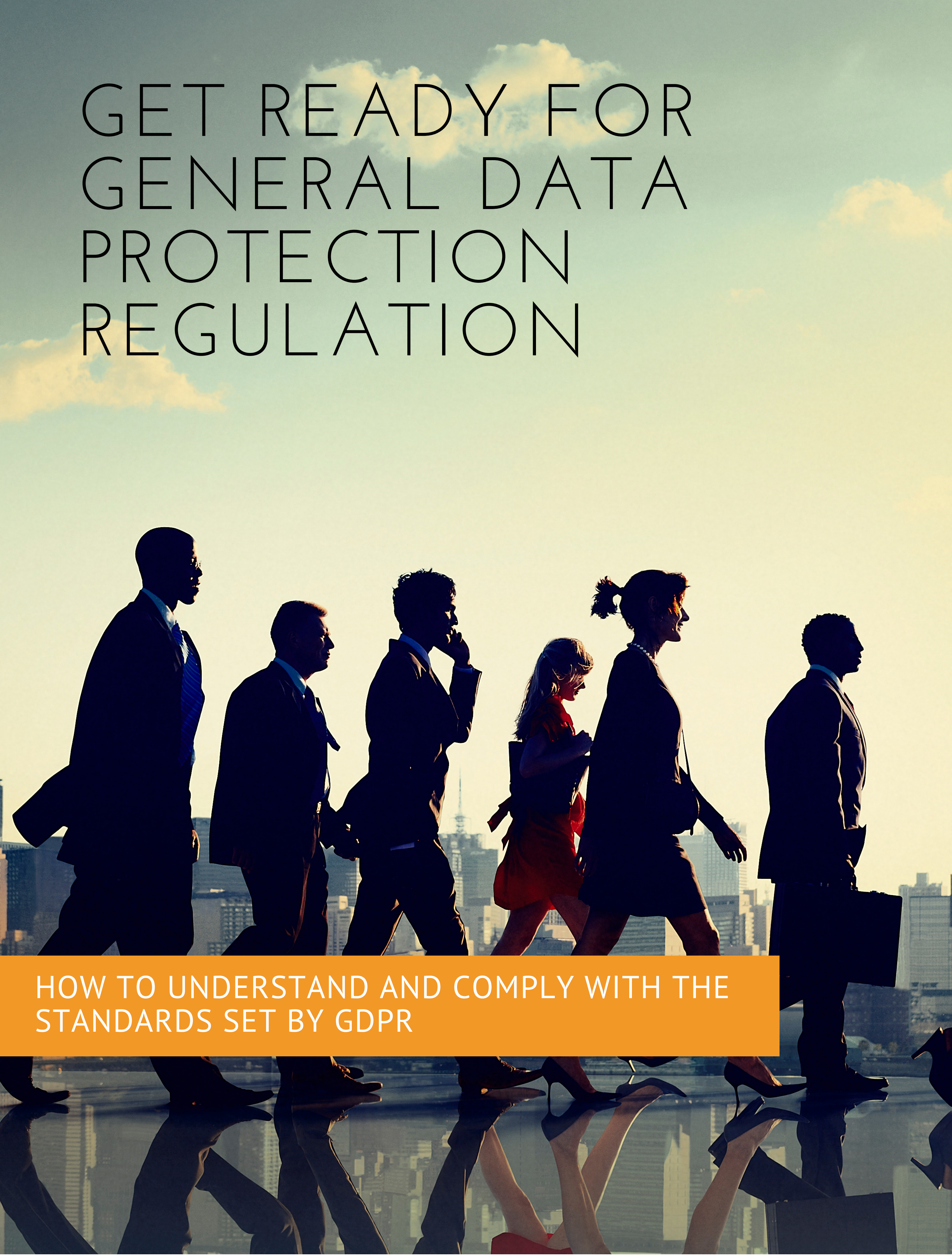
GET READY FOR GENERAL DATA PROTECTION REGULATION



HOW TO UNDERSTAND AND COMPLY WITH THE STANDARDS SET BY GDPR

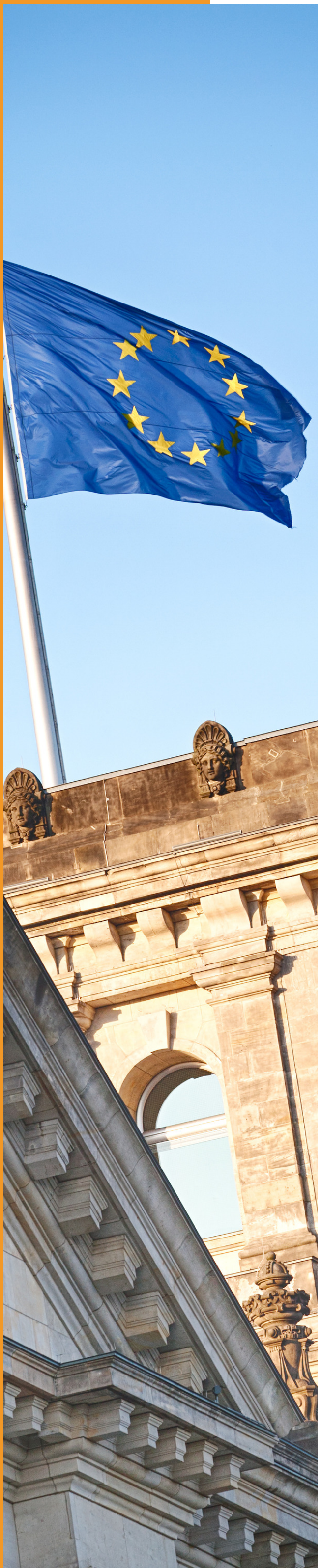
Awingu.com

One Workspace. Any Device. Anywhere.

Gartner Cool Vendor 2017

01

INTRO



After four years of preparation and debate, the GDPR was finally approved by the EU Parliament on 14 April 2016. It entered into force 20 days after its publication in the EU Official Journal and will be a direct application in all members states two years after this date. Enforcement date: 25 May 2018 - at which time those organizations in noncompliance will face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this white paper.

The EU General Data Protection Regulation (GDPR) consists of 99 articles that are grouped in 11 chapters.

02

THE BASICS OF GDPR

GDPR is a blueprint for a combination of legal, technological and work habit changes within an organization. It is not limited to one single process or team. It touches the entire organization. And that's why implementing the regulation often isn't straight-forward.

The regulation introduces the following four roles:

DATA SUBJECTS

The people whose personal data is collected.

DATA CONTROLLERS

The entity doing the data collection. It determines the purposes, conditions and means of the processing of personal data.

DATA PROCESSORS

The entities that process the collected information on behalf of the data controller. The GDPR places specific legal obligations on Data Processors; for example, the requirement to maintain records of personal data and processing activities.
Data Processors will have significant legal liability if responsible for a breach.

DATA PROTECTION OFFICER (DPO)

The DPO keeps management informed regarding their obligations under the Regulation, and is the primary contact for supervisory authorities. The DPO is not mandatory for all companies. It can be an external advisor (e.g. lawyer or consultant).

03

RIGHTS OF THE DATA SUBJECTS*

Already prior to GDPR, local regulators covered privacy (e.g. Belgian Privacy Act for Belgium). GDPR now expands these local regulations. Typically, national privacy regulations would cover:

- **The right to be informed** (Privacy Policy): Personal data must not be processed without the Data Subjects' knowledge. When personal data are collected, the data subjects have to be informed of the purpose of the collection. The Privacy Act stipulates which data have to be provided. This formality has to be complied with regardless of whether the data were obtained from the Data Subject or indirectly.

- **The right of access**: Any person has the right to obtain an extract of the data being processed in an intelligible form, as well as all available information on the origin of the data. The right to know the origin of the data is particularly important, as it is especially this question that is relevant to Data Subjects.
  It is possible for a decision having far-reaching consequences for the Data Subject to be taken solely on the basis of an automatic processing operation (this may be the case for loans or insurance policies). The Data Subject must then also be able to access the logic the automatic processing is based on.

- **The right of rectification**: Individuals can have incorrect data relating to them rectified free of charge, and have incorrect, irrelevant or incomplete data erased or prohibited. Controllers must answer the individuals having requested the rectification within one month. They have to mention what has been rectified or erased. If not, Data Subjects can address the Privacy Commission to submit a complaint. They can also bring the case before a court.
  If incorrect, incomplete, irrelevant or prohibited data have been disclosed to third parties, the controller must inform the recipients of the data of the rectifications or erasures within one month, unless it is impossible or extremely difficult to do so.

- **The right to object:** Individuals have the right to object to the processing of data relating to them but have to have serious and legitimate reasons to do so. The right to object is not granted for a processing operation that is necessary to enter into or perform a contract; it is also impossible for Data Subjects to object to the processing of their data if it is imposed by a legal or regulatory provision. If the data are collected with a view to direct marketing (including publicity), Data Subjects can object to the processing free of charge and without reason.

* https://www.balabit.com/blog/gdpr-the-basics/

04

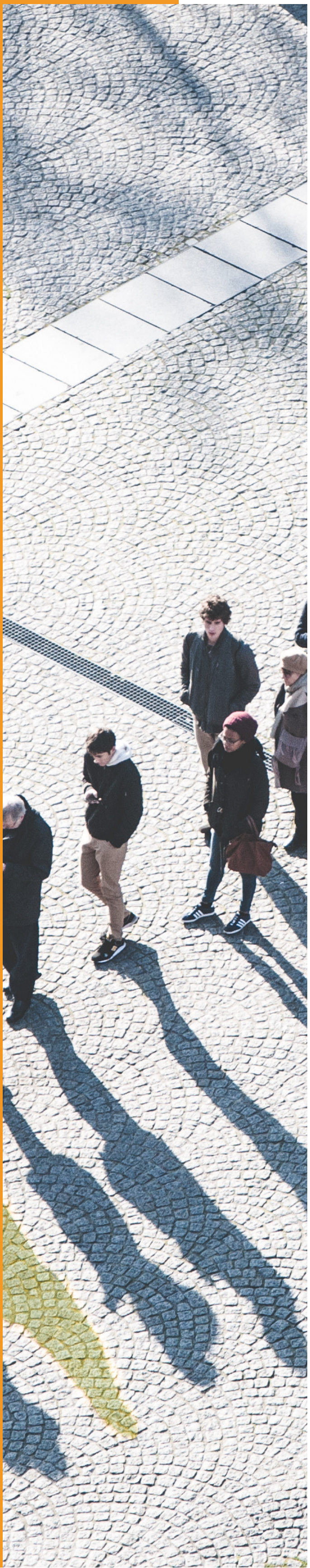
RIGHTS OF THE DATA SUBJECTS*

GDPR will give Data Subjects – you and me – a number of extra rights to which businesses must comply. These include:

- **The right to withdraw the consent**: It must be as easy to withdraw consent than as it is to give. Once consent is withdrawn, this not necessarily means the data is deleted.
- **The right to be forgotten**: Next to the right to withdraw the consent Data Subjects have the right to have their personal data erased and no longer used for processing.
- **The right to the restriction of processing**: Instead of requesting erasure, a Data Subject can also request a restriction of the processing of personal data. Where processing has been restricted, the data controller can in principle only store the personal data. Any further processing is only possible with the consent of the Data Subject or in a limited number of situations expressly listed in the GDPR. (eg. for legal reasons)
- **The right to data portability – "backpack"**: New under the GDPR is also the right to data portability. When personal data is subject to automated processing on the grounds of consent or a contractual agreement, the Data Subject is allowed to request that the controller provides a copy of the data concerned in a structured, commonly used, and machine-readable format. This is meant to allow the Data Subject to transmit those processed personal data to another controller (of his choice) without the hindrance of the controller that collected the data in the first place.
- **The right not to be subject to automated decision-making (profiling)**: Profiling is composed of three elements: it has to be an automated form of processing, it has to be carried out on personal data and the purpose must be to evaluate personal aspects about a natural person. Companies will then need to ensure that their profiling activities have a legal basis: 1/ the existence of a law authorizing such processing; 2/ the necessity of such processing to execute or perform a contract with the Data Subject; or 3/ the Data Subject's prior consent.
- **The right to be notified in case of a data breach**: Before the GDPR there were no obligations on data processors to notify data breaches. The GDPR enforces the right to be notified in case of a personal data breach. This must be done to the supervisory authority or the individual when there is a high risk to their rights and freedom. This notification needs to happen within 72 hours and contain the nature of the data being breached, including, where possible, the categories and approximate number of Data Subjects and personal data records concerned, the name and contact details of the DPO and the measures taken or proposed to address the breach and/or mitigate its effect.

* https://www.balabit.com/blog/gdpr-the-basics/

05



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS*

Data controllers and processors will have a number of responsibilities to comply to also. These include:

- **Accountability for violations and breaches**: Both controllers and processors can be held responsible by the supervisory authority in the event of any negligence of personal data security or not complying with the GDPR requirements.
- **Embedded security measures**: The security of personal data should be in the DNA of the infrastructure. All flows and data stores need to be built with the focus on security
- **Visibility in the data flow**: Information and the actions executed to it must always remain visible and traceable. Controllers and processors need to have a data flow mapping which allows inventory of all personal data.
- **Full functionality of data handling**: All implemented habits and technologies must serve the sole purpose they were intended for.
- **End-to-end security**: Not allowing any gaps during the data handling process. Constantly managing the security of information and the actions taken by users allowed to control the data flow.
- **Privacy by default (or by design)**: Once an agreement has been made between the subject and the other data entities, divergence from the terms is only possible once an additional agreement has been made by the parties.

* https://www.balabit.com/blog/gdpr-the-basics/

07

ACCOUNTABILITY OF DATA CONTROLLERS AND PROCESSORS

The controller shall be responsible for the processing and shall be able to demonstrate compliance with the GDPR.

The dynamic and permanent process of taking the appropriate technical and organizational measures in order to ensure/be able to prove that the processing is done in compliance with the GDPR.

Data controllers can ensure the protection of personal data and demonstrate compliance with the GDPR by performing a Data Protection Impact Assessment (DPIA).

According to the guidelines in the article 29 Working Party* the minimal content of DPIA is:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data.
- The measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

* Wikipedia writes: The Article 29 Working Party (Art. 29 WP) is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The composition and purpose of Art. 29 WP was set out in Article 29 of the Data Protection Directive, and it was launched in 1996.
Its main missions are:
• Provide expert advice to the States regarding data protection
• Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland
• Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data
• Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community

08

ACCOUNTABILITY OF DATA CONTROLLERS AND PROCESSORS

WHAT COMPANIES ARE IMPACTED?

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU Data Subjects. It applies to all companies processing and holding the personal data of Data Subjects residing in the European Union, regardless of the company's location. (*)

WHAT DATA ARE WE TALKING ABOUT?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information or a computer IP address.

This is much broader than any information that is relevant to an individual. Any information that is specifically attributable to the user is considered personal data. (*)

WHAT IF YOU DON`T COMPLY?

"Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 million, whichever is higher. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and Data Subject about a breach or not conducting the impact assessment. It is important to note that these rules apply to both controllers and processors - meaning 'clouds' will not be exempt from GDPR enforcement." (*)

WHO NEEDS A DATA PROTECTION OFFICER (DPO)?

"One of the new obligations in the GDPR concerns the appointment of Data Protection Officers (DPOs). The concept of having a privacy professional to guide for compliance is nothing new in Europe but it was previously regulated at Member State level. There was no uniformity. (**) DPOs must be appointed in the case of (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO. (*) The criteria such as 'core activities' and 'large scale' can, however, be interpreted in a broad way as mentioned in the opinion Guidelines on Data Protection Officers ('DPOs'), wp243rev.01 of article 29 working party (**).

* http://www.eugdpr.org/gdpr-faqs.html
**http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

IS GDPR ALSO APPLICABLE FOR THE UNITED KINGDOM POST-BREXIT?

If you process data about individuals in the context of selling goods or services to citizens in other EU countries then you will need to comply with the GDPR, irrespective as to whether or not the UK retains the GDPR post-Brexit.

If your activities are limited to the UK, then the position (after the initial exit period) is much less clear. The UK Government has indicated it will implement an equivalent or alternative legal mechanism. Our expectation is that any such legislation will largely follow the GDPR, given the support previously provided to the GDPR by the ICO and UK Government as an effective privacy standard, together with the fact that the GDPR provides a clear baseline against which UK business can seek continued access to the EU digital market. (*)

* http://www.lexology.com/library/detail.aspx?g=07a6d19f-19ae-4648-9f69-44ea289726a0)

EGENT STREET W.I.
極度乾燥(しなさい)
Superdry
ORLEBAR BROWN
REISS

HOW TO GET STARTED?

STEP 1: CREATE AWARENESS

STEP 2: GET YOUR ORGANIZATION READY

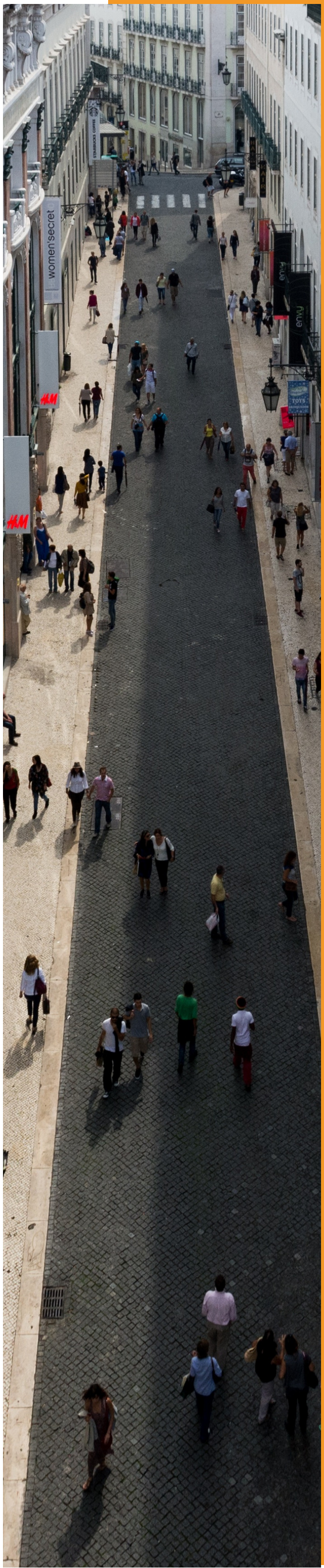
STEP 3: CREATE A DATA MAP

STEP 4: IDENTIFY WHAT DATA YOU NEED TO KEEP

STEP 5: PUT SECURITY MEASURES IN PLACE

STEP 6: REVIEW YOUR (DATA SUBJECT FACING) PROCESSES

HOW TO GET STARTED?



1. CREATE AWARENESS

The first step towards making sure GDPR is implemented is making sure it gets the correct platform within an organization. An absolute minimum is to make sure the management team is involved. In later phases, the rest of the organization should be informed and involved.

2. GET YOUR ORGANIZATION READY

The setup of GDPR comes with the setup of some formal roles such as a Data Protection Officer. Assign these roles earlier rather than later. In parallel assign a member of the management committee as a sponsor for a GDPR implementation. It will help enforce the right level of priority and effort is given to GDPR. Typically, the sponsorship role can be taken by the CIO or even CEO.

3. CREATE A DATA MAP

Once the project governance for GDPR is established, the real work will begin. Start mapping where 'personal data' (Data Subjects) is used throughout your entire business are used. What is it? Who has access to it? What is the level of risk associated with this data? Where is it? Is it based on a central database, or are there copies in multiple locations? Many tools (from basic excel templates to advanced software) exist to help in this process.

4. IDENTIFY WHAT DATA YOU NEED TO KEEP

We all tend to 'hoard' data from customers as they might be handy at one point or another. Not so in a GDPR world. You won't be allowed to keep more personal information than needed, and, you won't be allowed to keep this data 'at eternum'. GDPR will encourage a more disciplined treatment of personal data.
In the clean-up process, ask yourself:

- Why exactly are we archiving this data instead of just erasing it?
- Why are we saving all this data?
- What are we trying to achieve by collecting all these categories of personal information?
- Is the financial gain of deleting this information greater than encrypting it?

5. PUT SECURITY MEASURES IN PLACE

You need to put all levels of security in place to make sure your company's data is secure from breaches. This is translated into the implementation of IT best practices. The use of 'multi-factor authentication' to login into your applications and data, for example, is seen as an absolute minimum.

In parallel, structures must be put in place that allows you (oblige you) to notify individuals and authorities in the event of a breach. These structures include the setup of tools that help identify if data breaches took place. These security measures need not only be in place within your company but also with your vendors. Outsourcing your IT activities, for example, doesn't exempt you from being liable. Extensive checklists exist to guarantee GDPR compliance from your vendors. We much like the check list from BELTUG (www.beltug.be).

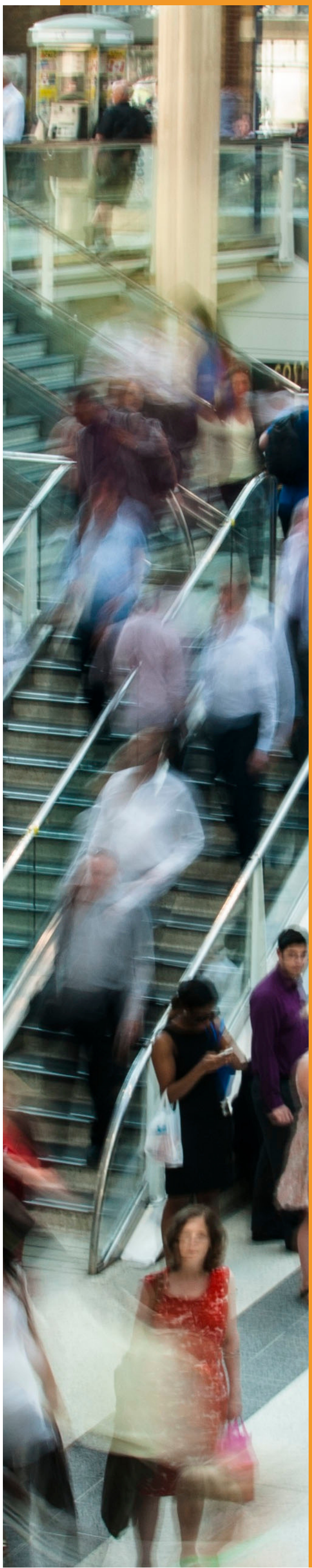
6. REVIEW YOUR (DATA SUBJECT FACING) PROCESSES

"Data Subjects" have a set of basic rights under GDPR. As a business, you will need to make sure you can comply to exercising any of these rights, e.g:

- What is the process if an individual wants his data to be deleted?
- How can you make sure deleting data is done across all platforms?
- How do you 'transfer' data if a Data Subject requests so?
- What is the communication plan in case of a data breach?

Furthermore, individuals need to give explicit consent to the use of their data. This means 'pre-checked' boxes will no longer be accepted. Businesses will need to be explicit on how this information will be used. The contact data of someone that signs-up to join an online webinar, can not be added to the newsletter distribution list for example. This will also apply to the 'cookie' tracking tools that all of us use today on our websites. This also means you will have to review all of your privacy statements and disclosures and adjust them where needed.

WHAT DOES GDPR MEAN FOR MARKETING AND SALES?



The way we – or at least some of us – do sales and marketing will be dramatically impacted when GDPR is in effect. Our approaches for inbound and outbound lead-generation (and nurturing) will be impacted and will need, at a minimum, fine-tuning.

Especially Article 4 of the GDPR will have a big impact on marketers. Article 4 defines consent as: "...any freely given, specific, informed and unambiguous indication of his or her wishes by which the Data Subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

Let's have a look at some areas where Marketing and Sales will be impacted:

INBOUND LEAD GENERATION

Businesses have created many ways to gather email addresses: online trial accounts, gifts, webinars, whitepapers, conferences,... In GDPR this will still be possible, but the Data Subjects will need to give 'explicit' consent on how their contact data can be used. That means: 'opt in' instead of 'opt out', and, you will need to clearly describe how this personal information will be used. You cannot send your weekly newsletter to somebody that signed-up for an online trial account. This same process applies to cookies and online tags. Clearly, this will impact how we do outbound marketing and sales significantly.

CONSENT MANAGEMENT

Data Subjects get the right to change the consent they have given you at any time. In other words, a platform or process needs to be in place and where the Data Subject (for example a hot lead of yours) can manage how you will reach him. E.g. he might have given initial consent on the weekly email newsletter and an online trial account, but he might want to ditch the newsletter after the first week. The platform must be in place, and, the marketing automation setup appropriately.

DATABASE PROVIDERS

We've all been tempted one time or another to buy a database with contact information. In the era of GDPR, this will be almost a de facto no-go zone. Data Subjects will need to give explicit consent to your company to be contacted. You will be responsible for the databases and need to know where the database came from, who gathered it, and, what storage duration period was communicated.

ONLINE RETARGETING

Retargeting has become a best-practise. With retargeting, marketers will try to provide relevant advertising to visitors of its website (or social media channels). If Data Subjects do not give explicit consent, then retargeting can only be used in a very generic way without any profiling. Marketing automation as a whole will get a lot more difficult to implement correctly.

WEB ANALYTICS

Any website owner these days will leverage web analytics tools such as Google Analytics. At the heart, these tools only provide an aggregated view of data which is OK from a GDPR perspective. However, most of these tools will also provide some degree of profiling and analysis on the profiling. This will only be possible with an explicit consent (that is: "opt in") from the Data Subject visiting your website. In other words: if you've lawfully collected data from a certain amount of customers and want to use that data analytically to derive shopping habits and create sales personas, then you need to have consent to do so (and if you haven't included 'profiling' in your original consent statement, then you need to collect a new one). If someone declines, you'll need to withdraw those particular sets of data from your analysis.

Where the above seems to suggest this is only applicable online, it is not. There will be a need for 'proof' also in the case of physical meetings for example. As a result of this, data (think about your lead lists) will start shrinking as of 2018 when people start using their right to be forgotten. Businesses will need to find new ways to create leads and engage with them, similar for nurturing existing customers. Probably a new mix of classic advertising, press, social media influencers and advanced online engagement will emerge, where the weight of the latter might (or might not) decrease.

16

HOW CAN AWINGU HELP YOUR BUSINESS BECOME GDPR COMPLIANT?

GDPR clearly touches any business at its core. Processes, documentation, organization, IT tools, etc. - all are impacted.

Awingu is not the ‘one-size-fits-all’ solution that will magically make your business GDPR ready. Yet, businesses that adopt Awingu will already be able to take some significant steps towards compliance.

We’ve grouped how Awingu can help your business along the 6 readiness steps shown on the table on the next page.

GDPR READINESS STEP	CAN AWINGU HELP?
1. CREATE AWARENESS	Not applicable
2. GET YOUR ORGANIZATION READY	Not applicable
3. CREATE A DATA MAP	**Centralize Data** Awingu won't help businesses in their initial data mapping. However, Awingu does help in keeping a central repository of data. Since Awingu runs completely in the browser there is no local footprint on the end device. Files and applications remain in the safe realm of the enterprise. Due to this nature, we have automatically increased protection against (ransomware) viruses.
4. IDENTIFY WHAT DATA YOU NEED TO KEEP	Not applicable
5. PUT SECURITY MEASURES IN PLACE	**Secure login** The setup of "Multi-Factor Authentication" (MFA) before accessing applications or data with sensitive data is considered a bare minimum. Awingu comes out of the box with the possibility to enable Multi-Factor Authentication. This can be the built-in One Time Password solution or by integrating with various 3rd party MFA providers such as Duo Security and SMS Passcode. Awingu's built-in solution is available at no extra cost. **Encryption** All data communication via Awingu can be encrypted. Businesses can use their own SSL offloader or leverage the built-in SSL offloading capability of Awingu. Again, this is available at no extra cost. **Shadow IT** (*) Awingu allows to share files and applications and enabling bringing this to any device. The need to use 'shadow IT' tools (e.g. the popular WeTransfer, or just an email to a private account) is no longer there. **Centralize Data and no local data** Awingu won't help businesses in their initial data mapping. However, Awingu does help in keep a central repository of data. Since Awingu runs completely in the browser there is no local footprint on the end device. Files and applications remain in the safe realm of the enterprise. This means that if a device is lost or gets stolen, there is no risk of losing data that would be locally stored on the device (as there is none). Furthermore, due to this nature, we have automatically increased protection against (ransomware) viruses. **Usage Audit and anomaly detection** Awingu keeps track of logins, application sessions, connected SaaS sessions, shared files, allowing to detect anomalies and alert in case of. This comes out-of-the-box and at no extra cost. **Keep using existing devices** Awingu runs in the browser of any device. These devices don't even need to be "managed" by the IT department, nor do they need to run on a similar version of Operating System. In short: with Awingu, GDPR can be implemented without large impact to the end-point (device) side.
6. REVIEW YOUR (DATA SUBJECT FACING) PROCESSES	**Centralize Data** Awingu makes working with one single and central data repository easy, also for mobile workers and even on any type of device. Moving 'Data subject's data or erasing it will be easier, given there is only one source. Data does not reside on end-user devices etc.

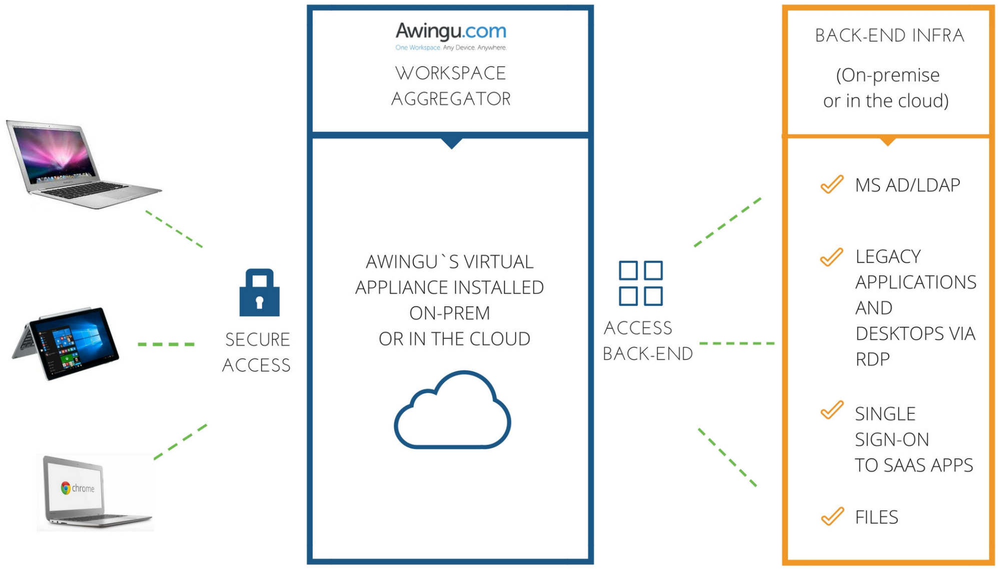
* Wikipedia, July 2017 defines shadow IT as: IT is a term often used to describe information-technology systems and solutions built and used inside organizations without explicit organizational approval. It is also used, along with the term "Stealth IT", to describe solutions specified and deployed by departments other than the IT department.

HOW DOES AWINGU WORK?

Awingu is deployed as a virtual appliance on most hypervisors, in a private or public cloud. From there, Awingu will connect into a classic back-end environment.

- ➢ It will link with Active Directory or LDAP for user management.
- ➢ It will connect to application servers running Microsoft RDS for legacy applications, Windows applications and/or desktops.
- ➢ It will set up a Single-Sign-On with SaaS services.
- ➢ Finally, it will connect to classic file systems via WebDAV and CIFS and with cloud storage environments such as Microsoft's OneDrive.

For end-users, everything is available in a browser via Awingu's online workspace. No need to install agents, plug-ins etc. Any device with a recent browser can be used securely - this includes private or unmanaged devices.


Awingu.com
One Workspace. Any Device. Anywhere.
WORKSPACE AGGREGATOR
AWINGU`S VIRTUAL APPLIANCE INSTALLED ON-PREM OR IN THE CLOUD
SECURE ACCESS
ACCESS BACK-END
BACK-END INFRA
(On-premise or in the cloud)
✓ MS AD/LDAP
✓ LEGACY APPLICATIONS AND DESKTOPS VIA RDP
✓ SINGLE SIGN-ON TO SAAS APPS
✓ FILES

To put it simply, Awingu will (1) aggregate applications and files, (2) act as an HTML5 gateway for applications and desktops running on the applications servers and (3) act as an Identity provider.

In terms of scalability, Awingu is 'stackable'. Our guidance is to host up to 100 concurrent users on one single Virtual Machine and simply add Virtual Machines for additional users. Finally, Awingu's software is multi-tenant, can connect with multiple Active Directories, can be branded, and is open API based. As such, it is also a Service Provider-ready solution.

TRIDENT
TRIDENT

ABOUT THE AUTHORS

ARNAUD MARLIÈRE in

Arnaud is Chief Marketing Officer for Awingu. Prior to joining Awingu, Arnaud worked at Belgacom (the Belgian incumbent Telco) and 'The Boston Consulting Group'.
During his time at Belgacom, Arnaud was heading the cloud product management activities and launched multiple cloud-based solutions: IaaS, Office 365, e-commerce, Dynamics CRM,...He has lived 'first hand' the challenges of bringing to market a SaaS service. At the Boston Consulting Group, he got involved in the firms' IT practice and the complexity of IT in large enterprises. Arnaud is passionate about cloud, mobile, ISV's and the indirect channel.

PIETER DE CLERCK in

Pieter is in charge of Evangelisation and Business Development at Awingu. Passionate about technology, Cloud, automation and Internet of Things, Pieter has a long work experience as engineer, managing several engineering teams and as CTO. Being at Awingu since the very start, he has a very deep insight in how Awingu works. As security is one of the most important features of Awingu, he added GDPR to his research and participated in relevant seminars and conferences.

ABOUT AWINGU

Awingu develops software to simplify enterprise mobility and liberate legacy applications. Our software aggregates all company files and applications to one secure online workspace that can be accessed from any device or OS using any HTML5-based browser. Awingu mobilizes all company applications without disrupting how you run your IT and works with any cloud service. No agent is required on personal or corporate devices, and collaboration and file sharing are as simple as sending a URL. IT assets remain centrally secure and no data footprint is ever left behind for a safe way to implement BYOD. Awingu is the fastest and easiest way to empower a mobile workforce. Awingu is headquartered in Ghent, Belgium with affiliate offices in San Francisco and New York. Gartner named Awingu as a ‘Cool Vendor’ when it released its “Cool Vendor in Unified Workspaces 2017” report.

Visit www.awingu.com or follow us on Twitter, Linkedin and Facebook.

Awingu.com

One Workspace. Any Device. Anywhere.

EMEA HEADQUARTERS

Awingu N.V.
Ottergemsesteenweg-Zuid 808 B44
9000 Gent
Belgium

+32 9 296 40 11

info@awingu.com
VAT NUMBER: BE 0832 859 222

US OFFICES

Awingu Inc.,
7th floor, 1177 Ave of the Americas,
NY 10036, New York
info.us@awingu.com

Awingu Inc.
620 Davis Street,
CA 94111, San Francisco
info.us@awingu.com