GDPR FOR
UNSTRUCTURED DATA

xenit
return on content

7 CHALLENGES FOR SECURING YOUR DOCUMENTS

In collaboration with

CUSTOMER
DRIVEN IT
CDI-PARTNERS.BE

DISCLAIMER

This white paper is a commentary on the GDPR, as Xenit interprets it, as of the date of publication. We've spent a lot of time with GDPR and like to think we've been thoughtful about its intent and meaning. But the application of GDPR is highly fact-specific, and not all aspects and interpretations of GDPR are well-settled.

As a result, this white paper is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR might apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance.

Published
March, 2018
Version 1.0

INTRODUCTION

Beginning on May 25, 2018, the General Data Protection Regulation (GDPR) will implement a new legal framework in the European Union (EU) for the protection and distribution of personal data.
GDPR is becoming the most crucial regulation through EU's data privacy legislations, the due date is right around the corner and the penalties for non-compliance are severe (€ 20m or 4% of global annual turnover).
As the attention to the regulation is at the top, there is now a growing concern about GDPR compliancy by all organizations that are affected by it.
GDPR will increase privacy for individuals and organizations must implement capabilities to ensure appropriate rights and adequate protection to safeguard the privacy of those individuals whose data they control.
Companies have a general obligation to implement technical and organizational measures to show that they have considered and integrated data protection into their processing activities (ICO).

MISSION

Several companies may be well on the way to define how to handle GDPR compliance for structured data. But many companies still haven't come up with a good way to handle GDPR compliance for unstructured data..
This whitepaper provides the main information about unstructured data and the Xenit solution to manage documents under the regulation.

"Did you know that most of the data breaches reported are related to unstructured data?"

IN A NUTSHELL

The solution summary explains the high-level GDPR area that Xenit can solve, these can be further broken down to show what Xenit products can help in which area. In a nutshell, Xenit, together with Alfresco, the leading Content Services platform, can help you in:

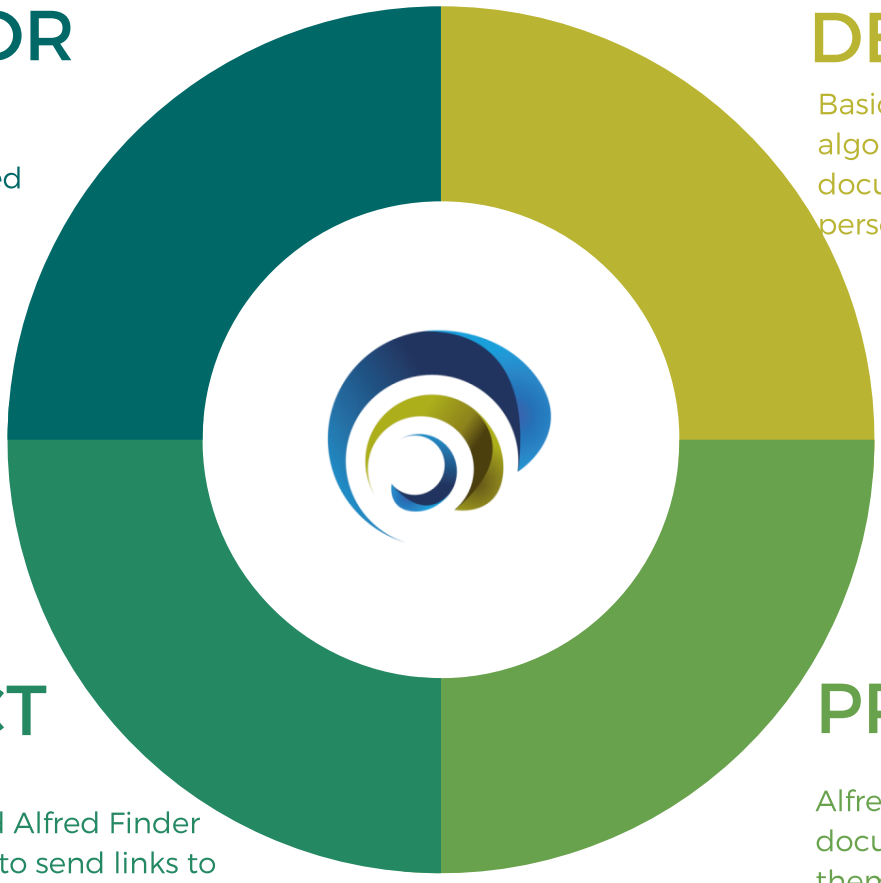
1. Discovering Personal Identifiable Information in documents
2. Tagging documents containing different types of Personal Data
3. Security rules based upon PII-type (No PII, PII, Sensitive, Medical, Criminal)
4. Monitoring and controlling

MONITOR

Within the Alfred Architecture, Alfred Edge to log every consultation

DETECT

Basic and most advanced algorithm to identify documents that contain persona; data



RESPECT

Alfred Desktop and Alfred Finder make it really easy to send links to documents and sharing them with a restricted audience

PROTECT

Alfred Archive to store documents, encrypt them

As there are no real examples of data breaches or other GDPR infringements, we have to look elsewhere if we want more insights in the effects of the GDPR. A good place to look for information is the United Kingdom. Although data breach notification is not mandatory, it is considered to be a best practice and close to 3000 breaches are reported each year.
Did you know that most of them are related to unstructured or semi-structured data? Documents, spreadsheets, mails and even paper files? One reason could be that it is far easier to properly protect data that are stored in databases, accessed through applications, than it is to have control over what happens to unstructured data.

Unstructured data are found everywhere, in emails and documents, stored on local or network drives, in the Cloud or on USB Keys. And they are easily copied and distributed. Unstructured doesn't mean chaotic. There can be a structure in the way the documents are stored, easy linking these documents to contracts, offers or individuals. And they are vulnerable. The most common type of data breach is sending these documents containing personal data to the wrong recipient by post, fax or email. Once an email has been sent it is impossible to control it, or is it?
Here a document management system comes in. You no longer send an email, you send a secure link and only users, with appropriate rights, have access.

But this is not the only advantage. Audit trail, usage tracking, retention policies, and legal archiving are just a few advantages that can easily be implemented with a document management system such as Alfresco.

20%

STRUCTURED DATA

Structured data refers to information with a high degree of organization, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search engine algorithms or other search operations. Structured data is relatively simple to enter, store (in database), query, and analyze.

80%

UNSTRUCTURED DATA

Unstructured data is more like human language. It is not stored into a relational database and the information does not have a pre-defined data model or is not organized in a pre-defined manner. Typical example of unstructured data is text.

GDPR 7 CHALLENGES

To make this very tangible, here are 7 challenges for securing your company's documents.

1. First, how do you know what documents to protect? How do you know they contain personal data?

2. Secondly, you have to adequately protect these documents.

3. Then, there is the aspect of responsibility: organisations must prove that they process personal data in a responsible way. And they need prove of having a legitimate purpose or consent to hold the document.

4. If data are on a portable device and it is important to work offline, how can this be protected?

5. And if something has gone wrong? How to know what data have been lost or stolen?

6. Personal data cannot be kept longer than necessary, or must be removed after a legitimate demand to be forgotten.

7. Sometimes it is needed to share documents with another party. How will you know who you have shared the document with and for what legitimate reason? And how to inform the 3rd party of a request to be forgotten?

"GDPR will touch every department, every function and every operation inside your organization. It will not only change the way you manage information, it will change the way people behave."

GDPR

7 CHALLENGES

for securing your company documents

1. Identify documents containing personal data and label them appropriately.

2. State of the art security of the documents and the metadata

3. Monitor and control access to the documents and store the right metadata to proof legitimate purpose.

4. Make documents available offline in a secure way.

5. Detect breaches and take appropriate action.

6. Keep track of the right time to delete documents and to permanently delete the documents so no backup copies exist.

7. Control the usage of documents by external parties.

CHALLENGE 1 - IDENTIFY DOCUMENTS CONTAINING PERSONAL DATA AND LABEL THEM APPROPRIATELY.

As we have seen, unstructured data are found everywhere, in emails and documents, stored on local or network drives, in the Cloud or on USB Keys. If we want to adequately protect personal data stored in these documents, the first hurdle to take is to know what kind of personal data is in which document. As documents are created or modified all the time, this classification has to be a recurring process. The results of the classification process must be stored in a such a way, security tools are able to use this information.

If we look at Alfresco, every change in a document – e.g. creation or modification – can trigger a policy that calls for the classification process. Then, the results of the process can be stored as metadata of the document. How this metadata has to be used will be described in Challenge 3 on page 14.

This process scans every individual file for personal data, regardless of the file type.

The most basic algorithm will search for structured data-types: National Number, Bank Account Numbers, Credit Card Numbers. This algorithm can be enhanced with company-specific structured data-types. For instance, Client Numbers that contain a check-digit.
A more advanced algorithm takes company-specific data as input and scans documents and files for this data. For instance, the names and addresses from the client database are used as input and documents that contain this information are flagged.
The most advanced algorithms use artificial intelligence such as natural language processing to search for certain data-types in plain text. This type of algorithm will return a probability. A threshold will have to be defined and tested on a representative random sample of documents.
Next to searching the content of the document, the type of document and the place it is stored can also be used: for instance, all documents in the folder 'employment contracts'.

The second part of the challenge was 'label the documents appropriately'. We have already mentioned that this information can be stored as metadata in Alfresco. We will keep whether the document contains personal data, if so, which type of personal data, the content found and, if possible, the link to the individual person.
As you can see, by using the classification algorithm we transform unstructured personal data into semi-structured personal data. The advantage is that we can implement more strict security on the documents and control how and by whom these documents are used. The disadvantage is that we have created more data that has to be protected.

CHALLENGE 2 - STATE OF THE ART SECURITY OF DOCUMENTS AND METADATA

When we store documents and other files, we not only store files that might contain personal data, we also create personal data by doing this.

When we run a classification algorithm, as discussed in the previous paragraph, we extract personal data from a document and store it in metadata. As a result, databases and indexes are filled with personal data in a semi-structured way. This makes finding and retrieving documents far easier, but it also increases the risk related with keeping personal data.

But there is more. Personal data is information related to an identified or identifiable natural person. For compliance reasons we will keep records of persons accessing, copying, and printing documents containing personal data. This audit trail links natural persons, for instance employees, to the documents they use. By definition, this information is also personal data.

And usage history is not harmless, it can lead to criminal convictions. In the UK there are some examples of hospital staff convicted for accessing medical files for non-professional reasons. This is in fact the very reason of keeping an audit trail, but unauthorized access to this information is a data breach in its own right.

Security of processing is covered in article 32 of the GDPR. We need to have appropriate security related to the risk to the rights and freedoms of natural persons. This is a very broad description that will lead to a lot of interpretation and discussion.

Typically, documents are stored on local or network drives or in the Cloud and distributed by email or by copying them on USB keys. Protecting documents in this way is not easy and options are limited to granting read or write access.

When we store documents in Alfresco, we gain a lot of options. Next to the original document, we can generate and store previews. These can even be personalized with a watermark. It is far easier to address people leaving documents on the printer (a possible personal data breach!) when their name is on every page.

Instead of sending documents by email, we will send links to documents or links to PDF previews. For very sensitive documents a separate login process can be enforced. This reduces the risk of sending documents to the wrong person (the number one type of data breach). And when a person asks to be forgotten, we can automatically inform the receiving third party of this request.

We will need to protect the documents, the database, the indexes, and the log files. For sensitive metadata, for instance the national number, we will use one-way encryption or cryptographic hashing. Only a user that knows the correct key can retrieve the documents related to the key, but the indexes can't be used to retrieve all the existing keys.

Documents stored in Alfred Archive are always protected and set up according best object storage practices. There is no direct access on a file system basis, which neutralizes 99% of known malware & intrusion risks. Furthermore, documents in the store are encrypted, with proper handling of the private and public key. Access to the document store is under detailed auditing. Life points can set the document to be 'immutable'. Moreover, a health processor continuously checks the binary integrity of all content - which can include the validity of a digital signature.

As for metadata, the database that contains the metadata can be encrypted on database level. Specific metadata fields with personal data can be encrypted and will not be exploitable by any direct access to the database. Index information is protected with encryption as well. No system can directly access the indexes in our reference architecture, as we have a safety gateway in front of the archive, and we have the Alfresco content services in front of the document store.

"Storing files and documents in Alfresco with Alfred Archive ensures adequate and appropriate security to your company's most vulnerable digital assets."

Alfred Archive Architecture

- Documents stored in **Alfred Archive** are always **protected** and set up according best object storage practices.
- There is **no direct access on a file system basis**, which neutralizes 99% of known malware & intrusion risks.
- Documents in the store are **encrypted**, with proper handling of the private and public key.
- Access to the document store is **under detailed auditing.**
- As for metadata, the database that contains the metadata can be encrypted on database level.

www.xenit.eu

xenit
return on content

CHALLENGE 3 - MONITOR AND CONTROL ACCESS TO THE DOCUMENTS AND STORE THE RIGHT METADATA

Organizations must prove that they process personal data in a responsible way. And they need proof of having a legitimate purpose or consent to hold documents containing personal data.

Organizations need to ensure that their data processing activities are carried out in accordance with the regulation. In particular, organizations should pay close attention to the principles of transparency and data minimization while implementing new data processing activities.

Article 24 states "...the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation".

Good security is just a first layer, preventing unauthorized access to the data. On top of that, companies must also have internal rules, written down in policies, how personal data is treated. And they must be able to demonstrate that these rules are followed.

When we store documents in Alfresco, we can use the metadata to control who has access to which document. And this can be far more granular than with traditional access rights. Not only the place the document is stored (e.g. the HR-network drive) or the type of document (e.g. a medical questionnaire), but also the content of the document can be used. A rule could be “Exclude all documents where the person requesting access is mentioned”.

These kinds of rules are of course highly dependent on the context of a company or even a specific process within that company. They can control access to specific documents or flag this type of behavior in the audit module. For instance, a local hospital lists all employees accessing medical files of famous patients. This list is reviewed by the management on a weekly basis. Excluding access would interfere with providing care in an emergency situation, but the staff knows that, without a legitimate reason, they face dismissal when accessing these files.

For documents, as for structured data (fields stored in databases), organizations must determine and communicate the lawful basis and the purpose for processing. When storing documents containing personal data in Alfresco, it is possible – and recommended – to store the lawful basis and a reference to the consent application as meta-data. When an opt-out is recorded, all documents that where dependent on the consent of a data-subject can be deleted with one simple instruction.

These functionalities are supported by Alfred GDPR. Alfred GDPR applies a double filtering for GDPR access control. First of all, classical Access Control Lists are used. They assign the right to view or modify documents to groups of users. Access control lists are the base permission management mechanism in Alfresco. Extending this to cope with GDPR would complicate matters a lot. Therefore, we have a filtering mechanism in Alfred GDPR that is based upon meta-data and GDPR roles. As an example, your organization can create a “GDPR sensitive” role, assigned to a limited number of people, and only they will be able to perform operations (consult or share) on “GDPR sensitive” documents.

xenit
return on content

DATA PROTECTION PRINCIPLES

GDPR PRINCIPLES AND IMPACT

Fair, lawful and transparent processing	Organisations have to take additional care when designing and implementing data processing activities.
The purpose limitation principle	Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
Data security	Controllers are responsible for ensuring that personal data are kept secure, both against external threats (e.g., malicious hackers) and internal threats (e.g., poorly trained employees)
Accountability	Under the GDPR, the controller is obliged to demonstrate that its processing activities are compliant with the Data Protection Principles.

CHALLENGE 4 - MAKE DOCUMENTS AVAILABLE OFFLINE IN A SECURE WAY

People use different devices for different purposes and in different circumstances. Think about your habits: when you work at the office or at home, writing documents and creating content, you will use a computer. But to consult these documents, for instance while you are traveling, you will use a tablet or a laptop.

Although increasingly more people are always connected, storing documents locally on a device is still a common practice. This implies that the protection of these precious documents depends on the security of the portable device.

When an unencrypted portable device – a smartphone or a laptop - is lost or stolen and when there is the possibility that this device contains files with personal data, you will have to report this loss as a personal data breach! The notification to the supervisory authority must contain a description of the likely consequences of the personal data breach. But, how many companies know which files are on which device? My guess, not so many.

So, the challenge has two aspects: how to store the documents in a secure way and how to keep control over these files once they are stored on a portable device.

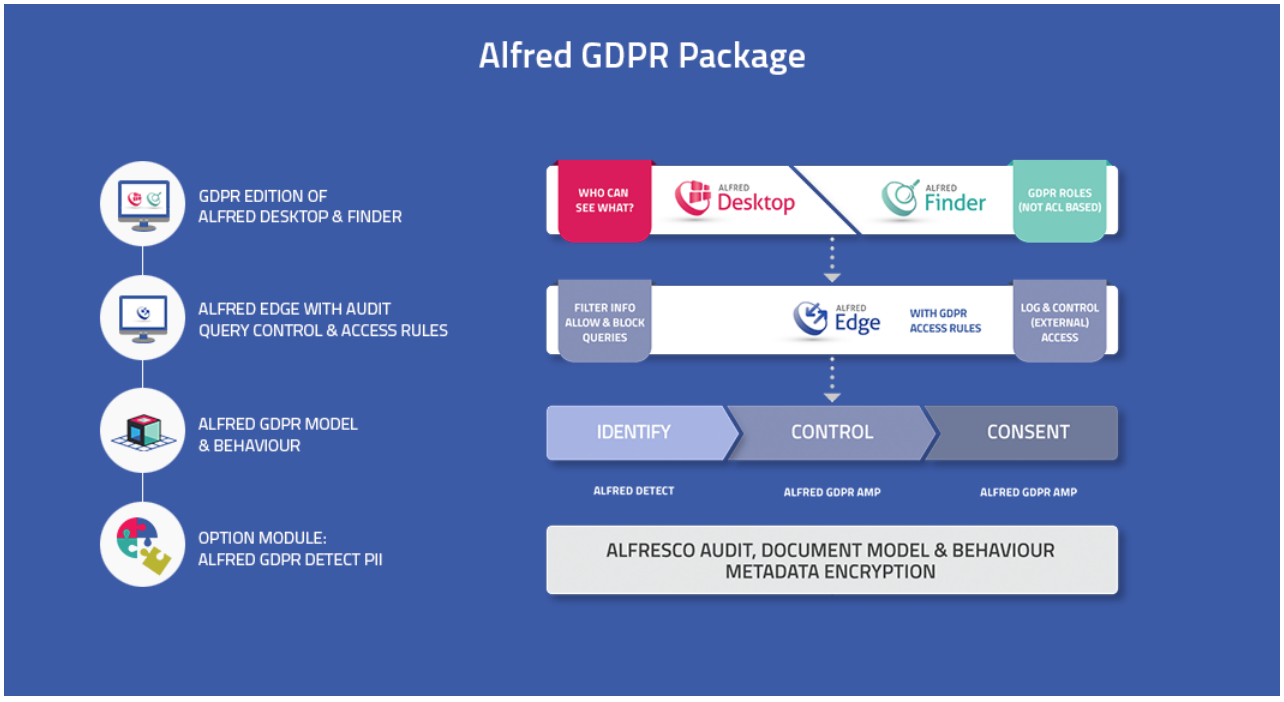
Securing the storage is not so hard if you can secure the device they are on. You can encrypt hard-disks and memory cards and protect access to the device by password policies. But what if you don't have control over the device?
And how can you know which files are on the device? And can you limit the possibilities to copy the files to another device like an USB-key or block sending these files by e-mail?

To face this challenge, Xenit is working on securing the content, through the Alfred GDPR Architecture and some features of the two products, Alfred Desktop and Alfred Finder, built on top of the Alfresco functionalities.

Alfred Desktop, a desktop application for Alfresco, keeps track of local content and removes it as soon as the user is done with it. For off-line editing and modification, working copies are created in a download directory. This working copy is under control of Alfred Desktop and it will only exist locally as long as it is needed. However, the corporate desktop policies remain important: local drives that can contain sensitive information should be encrypted at any time.

With Alfred Desktop and Alfred Finder, a web application for finding documents on an Alfresco back end, organizations can set a "GDPR download policy". In this policy, customers can enforce whether the original document format (Microsoft Office) or PDF should be downloaded.

Additionally, a watermark can be added to a downloaded file. Via the watermark, identification information is attached according to customer requirements. Typically, that covers “who” downloaded, a unique document ID, the GDPR categorization and it might contain consent information whether the document can be distributed outside of the organization. Alfred Edge allows to handle different types of access control to Alfresco: mobile users can have other policies than desktop users. We can disable downloading documents from a mobile device, but allow the previewing of such documents, while desktop users are allowed to download a document. Note that 'previewing' in many cases does an implicit browser download: customers that want to fully block such risk should explore pure 'streaming' solutions on top of our Alfred GDPR Architecture.



CHALLENGE 5 - DETECT BREACHES AND TAKE APPROPRIATE ACTIONS

Article 4 defines a Personal Data Breach as follows: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

A little quiz: What is not a personal data breach?

1. Someone accidentally deletes a document and there is no backup
2. Someone alters a document filled in by a client
3. A person sitting next to me on the train can see the screen of my laptop when I’m reviewing an employee file.

As you might have guested, all these could be Personal Data Breaches. And not all data breaches can be detected automatically. How would a system know a file is accidentally deleted or that you have left your laptop unattended without locking the screen? To minimize these types of risks, you need to set up internal policies and create awareness, by training and a lot of communication.

PERSONAL DATA BREACHES

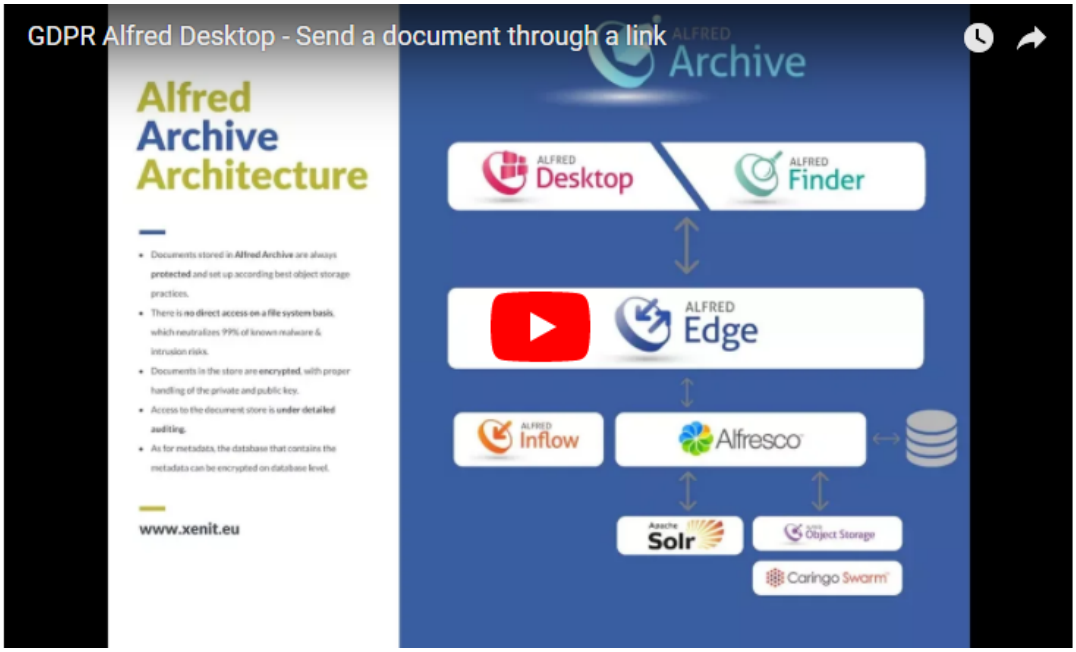
WHAT	The personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
WHEN	The GDPR explains that you need to notify a data breach if there is a risk to the rights and freedoms of individuals. For instance, the breach may lead to physical, material or non-material damage for data subjects such as: discrimination, identity theft or fraud; financial loss; or damage to reputation.
WHO	The supervisory authority must be notified. When the personal data breach is likely to result in a high risk, also the data subjects must be notified.
HOW LONG	The GDPR states that notification of a personal data breach to a supervisory authority must occur “not later than **72 hours after** the controller has become aware of it

xenit
return on content

A lot of breaches can be detected. And you will have to take measures to detect these. The higher the likelihood of breaches happening and the higher the impact of a possible data breach, the more sophisticated breach-detection must be.

Modern security systems search for uncommon behavior: signing in from Belgium and 10 minutes later from Singapore, downloading files in large quantities, using an unknown device. These are just simple examples; more sophisticated statistical analysis will search for patterns. Behavior that doesn't match these patterns is seen as suspicious.

Another technique is to use honeypot files: Files that only exist to be hacked. When such a file is touched, you know someone is in poking around in your system.
As mentioned before documents or more general files on network servers or local disks are difficult to control. If they can be copied onto a USB Keys or sent by mail, there totally out of control.
To mitigate the risk of local and email copies of privacy related documents, Alfred GDPR promotes and facilitates collaboration by sending links. No need to make or send copies of documents, but share by link.



Alfred Edge, an intelligent gateway, is the core of the Alfred GDPR architecture. All access to Alfresco is centralized in the gateway. The gateway defines a very narrow and business driven interfaces, with strict rules about what data and what queries different (GDPR) user profiles are allowed to access. All other other access to Alfresco is blocked.

All requests are logged and retained (with proper protection of private information!). Customers can then define breach patterns and have the gateway in real time filter and monitor for such behavior. Alfred Edge supports different interaction channels: intranet users, internet users, 3rd party systems. Using strong and positive identification, we then apply rules of expected behavior as defined by the customer.

Frequent access to private or sensitive documents can be detected and escalated. Searches on GDPR related meta-data (name, national id numbers) can be filtered, detected and blocked. If user x tries to access data about user y, e.g. via a broad query on the repository, we log and escalate such requests. Obviously, standard access control and GDPR roles will hide any information users are not entitled to access, but breach detection will bring such attempts to the attention of GDPR officers and DPO.

When the system becomes aware of a breach, different actions can be taken. The access to the system can be blocked, an alert will be shown on a console, an entry will be written in a log file. Which actions are appropriate depends on the sensitivity of the information in the system. In all cases, the breach has to be reviewed by the Data Protection Officer if there is one, or someone with a comparable responsibility, if not. Depending on their assessment, the authorities must be notified.

CHALLENGE 6- KEEP TRACK ON THE RIGHT TIME TO DELETE DOCUMENTS

At this point is quite evident how GDPR is an on-going process and companies have to put in place a long term plan to demonstrate their compliance. Another important change introduced by the GDPR is data minimization.

> "Keep only the information you need for as long as you need it."

This means, not only structured data (data in databases) must be deleted after a certain time, but also unstructured data has to be removed. Data and documents that are being kept on basis of consent must be deleted as soon as the consent is withdrawn.

As for the other challenges, implementing these functionalities on documents and files is more difficult than it is for structured data. Not only do you need to establish the right retention period, you need to keep this information with the document, and find a way to delete the document after the retention period has passed. We already talked about the need to keep a link to the consent that has been given in a previous paragraph.

In the simplest form, retention periods are fixed; you need to keep a document for x years. But it can become more complicated very fast. Keep the dossier (all the documents related to a certain contract) y years after the contract ends. In this case you could be obliged to keep certain documents for decades. The retention period is not fixed, but a rule. By consequence, you can't set the date of deletion the moment you store the file on your environment.

And deletion actually means removing all copies of the document from your system (and shredding the paper versions). For years companies are investing in backup solutions, so they can retrieve information that has been deleted. And now we need to find a way to selectively delete or at least block access to certain files on backups.

How simple would this be if we didn't store multiple copies of the same document on file servers and if we didn't keep back-ups.

Alfred GDPR helps to manage document retention, including GDPR related information. This means that the all GDPR aspect of your documents, including a clear view on PII (personally identifiable information) are under your control. Records management is the 'art of throwing away', so governance to remove sensitive information is as important as to retain information.

Building upon Alfresco Content Services, our powerful meta-data scheme allows to encode various GDPR retention and protection policies. Retention is ensured as long as consent is given. Once consent is withdrawn, a simple query allows to collect information to be removed. Needless to say that audit and protection mechanisms are provided to protect against any unintended operation.

Optionally, Alfred GDPR enables object storage for all your (GDPR) documents. By applying the proper versioning policy, and protecting against loss of documents via built-in (Geo) replication, there is no need for two or three tier back-up strategies. As a consequence, you have direct control over all documents and their history within one management layer. With smart versioning policies and object storage you simply eliminate the need to keep or clean back-ups.

Request a free day assessment

CHALLENGE 7- CONTROL THE USAGE OF DOCUMENTS BY EXTERNAL PARTIES

As we have seen documents, spreadsheets and other files are easily copied and shared across devices. This can be unwanted behavior, an employee copying customer data on a USB key before leaving the company, but mostly this is wanted behavior, working on a document with colleagues, sharing information within a department, sending out a work order to an external partner. And our seventh challenge is about the last example. How do you control information you shared with an external party?

Why would this be necessary? The most important article covering this situation is Article 19 "Notification obligation regarding rectification or erasure of personal data or restriction of processing. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."

When you share personal data with third parties, you should be able to notify them after a request for deletion or rectification. When you share structured data, this will almost always be done under a formal contract, transferring files or granting access to your databases through web services. Contracts should address the procedure to comply with Article 19.

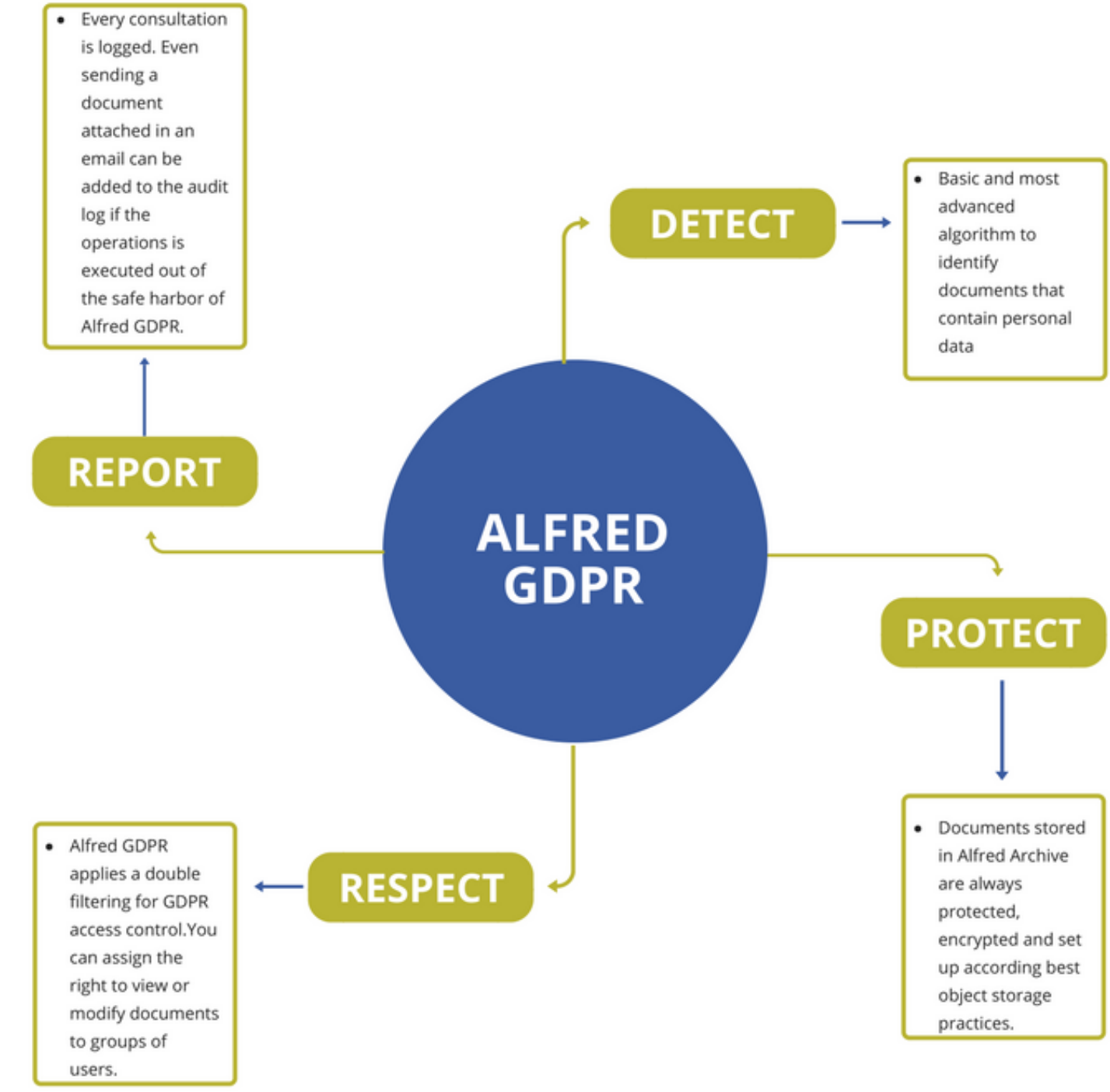
Sharing word or PDF documents and spreadsheets, will often be done in an informal way: by sending out emails or using file sharing utilities like Dropbox

So, when a data subject asks to be forgotten, can you inform all parties that have received information?

Once again, the solution lies in using a content management system. You stop sending out emails with documents, you share links to documents in your system. And not only can you keep track of who you shared the information with, you know if and when this party has read the document and if and when the information was downloaded. With this knowledge, you could even automate notifications after a request for deletion. If someone asks to be forgotten and the information was not downloaded, just revoke access rights. When the information was downloaded, send out a mail with the notification.

With Alfred GDPR we try, first, to minimize copies of documents, creating a single source of (document) truth which is easier to protect. Instead of email attachments to third parties, linking and sharing of documents are promoted and facilitated. With linking and sharing, full audit and access control are at your disposal. Tooling-wise, Alfred Desktop and Alfred Finder make it really easy to send links to documents and sharing them with a restricted audience. Downloads can be disabled, such that we only offer a service to consult the document, not to download a copy.

GDPR CHALLENGES FOR UNSTRUCTURED DATA



xenit
return on content

Alfresco allows to share a folder or a document with partners and people you assign. Using Alfred Edge's cloud authentication, these documents can even be shared outside your company walls with strong authentication for your external partners and customers. Links can entail strong authentication of the person accessing your document; we can make them secure, valid for a limited time and inside a specific geographic zone.

When employees, for good reasons, download a document for internal purposes, full audit information is available. Every consultation is logged. Even sending a document attached in an email can be added to the audit log if the operations is executed out of the safe harbor of Alfred GDPR.

Some previewers operate by downloading a document locally before displaying it. With streaming technology, a document never has to be downloaded, you can consult the content without a local copy. Alfred GDPR optionally offers such a streaming viewer if you need the additional protection. Last but not least, it is possible to watermark (PDF) documents such that there private or sensitive character is explicit and awareness about their private nature is increased. Water-marking is possible in preview and in the creation of a "GDPR protected PDF copy".

.

CONLUSION

Through the seven challenges, we have listed what you need to comply with the GDPR. Combined with unique GDPR functionalities of Alfred GDPR, Alfresco is the most appropriate environment to store, modify, archive, and delete your files. Alfresco is your chance to manage unstructured data under the regulation.

CONTACTS

Peter Morel

Sales Director and Co-Founder @Xenit

peter.morel@xenit.eu

Bart Van Bouwel

Managing Partner @ CDI-PARTNERS

bart.van.bouwel@cdi-partners.be

THANK YOU