windream GmbH – Whitepaper

The windream ECM System in the Context of the EU General Data Protection Regulation (EU GDPR)

windream GmbH, Bochum

windream GmbH
Wasserstr.219
44799 Bochum

Important note

All information and technical specifications in this book have been collected by the authors with great care. They cannot, however, either guarantee, take legal responsibility for or make any other warranty resulting from the use of this information.

We would also like to point out that all software and hardware logos and names are the exclusive property of the trademark, brandname or patent right holders. These are naturally protected by the appropriate laws and trade agreements.

Issue: 04/2018

Content

The windream ECM System in the Context of the EU General Data Protection Regulation (EU GDPR)

Important Note: This document exclusively applies to the contents of the EU General Data Protection Regulation (GDPR) and the "BDSG-neu" (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 bzw. Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU). Please always consider the domestic legislation or respective amendment acts based on the flexibility clauses of the EU GDPR of the specific EU member state. The legislation differing from the "BDSG neu" will not be topic of this document.

Management Summary

Summary of this document

Basically all companies are de facto affected by the requirements of the EU GDPR. In case of data protection violations, high fees may arise.

To be able to overcome the challenges of the regulation conveniently, the windream ECM System supports all users who deal with the EU GDPR. By means of specific use cases, this document points out how windream supports users even if the company has not, or only rudimentarily, dealt with the data protection regulations.

In this context, it is of great importance to use a system which is so intuitive to use that the user can continue to work as usual and does not have to get used to a new way of working. Exactly this requirement is fulfilled by windream completely.

Introduction

The EU General Data Protection Regulation (EU GDPR) is a regulation of the European Union, which standardizes the legal regulations for processing personal data by private companies and public authorities on an EU-wide scale. The regulation will become effective on May 25, 2018 and replace the previous regulation

"Bundesdatenschutzgesetz" (BDSG) (Federal Data Protection Act). The EU GDPR is binding for all member states of the European Union from this day on. The purpose of the regulation is to unify the protection of personal data within the European Union in a manner, which is legally binding for all member states.

The "New" Federal Data Protection Act

In the context of the new EU GDPR, the previously valid Federal Data Protection Act has been adapted to the EU GDPR. The reason for this change is that the EU regulation contains fifty so-called flexibility clauses. These clauses allow the EU member states to adjust their own data protection legislation to the EU regulation or to supplement them as long as these supplements do not conflict with the contents of the regulation. In Germany, these supplements consist of a reviewed version of the Federal Data Protection Act (Bundesdatenschutzgesetz), the so-called "BDSG-neu" (New BDSG), (official name: "*Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* bzw. *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU*") dated June 30, 2017.

Effects on Applicable Legislation

At this point of time, it is difficult to predict whether there will be a change in jurisdiction in the sector of data protection in Germany with the EU GDPR coming into effect or not, as the EU GDPR only replace the BDSG in the future. Of course, future jurisdiction will always be made based on the EU GDPR.

It can therefore be said, that the jurisdiction, until this point has been made based on the BDSG. Legal professionals predict that the current jurisdiction (not legislation) will continue to be made based on the BDSG and that future legal decisions which are passed based on the EU GDPR will in many cases refer to already made decisions based on the BDSG.

A legal commentary on the EU GDPR does not exist (yet)

As the EU GDPR will only become effective on May 25, 2018, no interpretations or commentaries on the regulation exist at present, although legal commentaries are of considerable importance in legal practice. Only once the EU regulation comes into effect, a jurisdiction which allows more precise and concrete interpretations of the EU GDPR will take shape.

Note: Another very important fact shall also be mentioned:

As with the BDSG, the regulations of the GDPR are only valid if they are not opposed by other laws or regulations (for example financial or fiscal regulations such as the GoBD (Grundsätze ordnungsgemäßer Buchführung/Guidelines on proper accounting) in Germany).

Effects on Companies

That the new EU General Data Protection Regulation will become effective at end of May 2018 should be a known fact in every company. According to the results of surveys conducted by various analysts, it cannot be expected that all companies are adequately prepared for the new regulation, although nearly all companies are affected directly by it. One reason for this certainly is that there is a general uncertainty of how and with what measures an implementation can be achieved lawfully. We want to react to that uncertainty with the present paper and show that windream will support users consequently with the implementation of the new regulations.

ECM Systems Offer Help

It is an often-overlooked fact that modern, IT-supported systems like windream exist, which not only support the data protection officer but all users in a company with the implementation of the requirements of the regulation. To guarantee the required protection of personal data, an ECM system like windream offers valuable help.

The purpose of the present white paper is to inform about the most important requirements of the new EU GDPR and to show how an ECM system like windream can help to fulfill the legal requirements.

Focus on Documentation Obligations

The mere fact that the regulation requires a comprehensive, transparent documentation of all processes involving personal data results in the requirement that the use of a specialized system for information management be the center of all activities. Here, "Enterprise Content Management" (ECM) with windream can show its full potential, especially if requirements such as limited access rights via a restrictive rights concept, complete traceability of document-related processes, or the adequate blocking or deletion of personal data are involved. All these aspects are directly connected with the requirements of the EU GDPR.

In the following sections, some examples are presented which are very concretely and directly connected with the single articles of the EU GDPR and show how the windream ECM system supports companies towards implementing the GDPR.

Complete Record of Processing Operations

Article 30 of the EU GDPR demands a comprehensive overview and description of all processing actions that are connected with personal data. This requirement is not new, as the BDSG, which will be valid

until end of May 2018 demands such an overview as well. However, article 30 specifies the contents, like, for example, names and contact data of the responsible persons within a company, the purpose of data processing, a description of the categories of affected persons and data, the categories of recipients and many more.

Data Categories, Document Histories and Record of Changes

For capturing and documenting these processes, windream is an excellent tool. That is not only true for the management of the process descriptions itself but also for a possible indexing of the process describing documents according to the data categories which are defined precisely in the regulation.

As far as changes or extensions of the existing documents that describe processing actions according to article 30 should be necessary, these changes can be proven by a complete document history. A good ECM system like windream can provide complete proof of changes or additions at any point of time "on demand".

Efficient Contract Management According to Order Data Processing (ODP)

The windream ECM system is able to manage and to systematically store even very special electronic data or document categories conveniently, for example contracts: "Contract management" is the key word here. The specific purpose is to create and manage electronic contract data in such a way that the documents associated with these data and their contents can be made available immediately. This especially applies to proof provided to the data protection authorities and for the fulfilment of article 28 of the EU GDPR.

ODP Contracts are Mandatory

For the case that companies – may it be as contracting authority or as subcontractor – process personal data on behalf of others, article 28 of the EU GDPR demands a comprehensive contract for every instance of order data processing (ODP). If an authority finds that no contract has been concluded for an instance of ODP, or that a contract cannot be found, the result can be, depending on the single case, a high fee.

By using the windream ECM system with its integrated contract management function this risk can be minimized significantly as the ODP contracts are safely archived in windream.

Both Contracting Parties Responsible

Another important piece of information in this context: The previously valid (until the end of May 2018) Federal Data Protection Act mainly

held the contracting authority responsible for controlling and complying with the data protection requirements by the contracting authority. The EU GDPR on the other hand holds both contract parties equally responsible. There is no more "difference in liability" between contract authority and contractor, another aspect which, at least indirectly, speaks in favor of using an ECM system for contract management on both sides.

The Aspect of Security in Data Processing

"Safety first" – that is what the GDPR demands in article 32. In this article, the technical and organizational measures a company needs to take to guarantee appropriate protection of personal data are described in detail. This requirement is already known from the Federal Data Protection Act but requires a complete documentation in the future as well.

The Documentation of Technical Organizational Measures

Technical organizational measures (TOMs for short) are usually constantly changing. The reason for that is that they need to be constantly adjusted, extended and changed, may it be due to new security measures within the company, due to an extension of the business location in connection with construction measures, due to a complete company relocation or due to modifications of the IT infrastructure.

windream offers the ideal function for documenting exactly these changes: the versioning of documents. This function allows users to maintain existing descriptions and to create new versions of the document before the document is changed or complemented by the description of new technical measures. In cooperation with the windream default function "Document History", a complete proof of when, by whom and to what extend the description of the technical organizational measures has been changed can be created.

Management of Declarations of Consent

According to article 6 ("Lawfulness of processing") and article 7 ("Conditions for consent" under (1)) the processing of personal data can also be authorized by a declaration of consent of the data subject. Article 7 (1) demands that the responsible party shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. The problem: The EU GDPR does not prescribe that a declaration of consent needs to be given in written form. But how exactly shall a consent be proven if not in written form? Therefore, it has to be said: without written consent, it is not possible to prove consent.

Reducing Administrative Effort

As experience shows, the management of the declarations of consent requires enormous of administrative effort. One cause for this effort is that consent always needs to be tied to a specific purpose, i.e. limited to a certain aspect of data processing (for example consent to the publication of employee photos in the intranet, consent to the publication of personal data in a newsletter and many more). Every change of purpose and therefore a "new purpose" requires gathering a new declaration of consent from every person involved.

An ECM system can, of course, not absolve a data protection officer from these duties, but it can be an enormous help in managing these declarations of consent, for example by systematically storing them in a personal register or in an electronic file (see above) in windream to which only the data protection officer has the access rights. The required rights for this purpose can be managed conveniently by using a rights concept within the ECM system. The windream ECM system solves this kind of problems as well.

The Right to Erasure and "to be Forgotten"

In general, according to article 17 of the EU GDPR, affected parties have the right to demand the erasure of their personal data where one of the following reasons applies.

Note: As already mentioned, the erasure of personal data is only justified if no other laws or regulations oppose this erasure (for example financial or fiscal regulations such as the GoBD in Germany).

While the right to be forgotten applies to "data that has been made public" "only", for example in social networks, data erasure from an ECM system can be, depending on the request, be automated as well. Apart from withdrawing all rights that allow access to the data, which will result in preventing all users from accessing the data, erasure can be achieved in other technical ways within the windream ECM system, for example via using an automated concept based on life cycle settings for documents. These settings allow automated deletion of data after a defined period of time, for example once the reason for the data storage has expired.

Logging Erasure Processes

In general, it can be said: the process of a data erasure needs to be logged as well. This requirement results from § 76 of the new BDSG, meaning the adjusted version of the BDSG, which the EU GDPR supplements and substantiates via a flexibility clause (as already mentioned above). § 76 specifies the logging of an erasure process as it

prescribes that only the data protection officer of a company is allowed to manage the logs of the erasure processes.

Responsibilities of the Administrator

This means that erasure log management cannot be the responsibility of an administrator. Without any doubt, the system administrator is of great importance when it comes to the IT infrastructure of a company, as he or she is responsible, for example, for data repository, data security, data availability, system maintenance and therefore for the erasure processes "per se". This position, however, should be strictly separated from the responsibilities of a company data protection officer.

Background: Fundamental Knowledge on the Topic of Erasure and Compliance

Generally, the idea of deleting data contradicts the purpose of compliant archiving where deleting or manipulating documents of all kind should be avoided. The key words here are "completeness", "unchangeability" and "prompt locating/fast accessing". To achieve that, windream uses many different mechanisms to ensure these aspects and to avoid unauthorized erasure. This is especially true for tax-relevant documents, credit cards and for complying with the GoBD requirements for which compliant storage is necessary.

This situation is made even more difficult by that there is no specific definition within the tax law stating which documents are tax-relevant and which are not. This serves to ensure, that the tax authorities can declare a document as tax-relevant at any time.

For that reason, it is important to check **before** deleting data whether the planned deletion process according to the EU GDPR is opposed by another legislation, which would make an erasure inadmissible.

Conflicting Legislations

As just mentioned, the retention obligation applicable to tax-relevant documents opposes the "right to be forgotten/right to erasure" specified by the EU GDPR. And that is just one open conflict of many.

Important Note: At this point, the EU GDPR DSGVO is very explicit and states that in the case of such a conflict with another legislation, the right to erasure of the data expires.

The Term Erasure

If a document is erased from a normal data system, the document is (in Windows) first moved to the recycle bin and can still be recovered from there. If the document is erased from the recycle bin, the link to the document is deleted from the directory on the hard drive as well. The document is not listed in the system and therefore not accessible

by regular means anymore. That means: after the erasure process the data is still existent, but has officially been "erased".

The previous jurisdiction based on the BDSG interpreted this process in the same way. The process of "erasure" should therefore be seen rather pragmatically and it cannot be expected that this will change significantly under the EU GDPR.

The Conflict between Erasure and Backup

When it comes to highly sensitive systems, there is a special definition of erasure processes. See also: https://www.haufe.de/unternehmensfuehrung/profirma-professional/dateien-und-datentraeger-sicher-loeschen-3-standards-und-verfahren-zum-sicheren-loeschen_idesk_PI11444_HI2288085.html.

Under this link, various default methods are described which allow secure erasure, for example in accordance with the guidelines of the BSI (Bundesamt für Sicherheit in der Informatik/Federal Office for Information Security).

Another problematic aspect in a strict interpretation of the term erasure are backups. From backups, the information to be erased needs to be deleted as well, which on one hand is technically very hard to achieve and on the other hand would mean an enormous amount of effort making it nearly impossible.

An "Austrian" Approach to Conflict Resolution

An approach from Austria could relieve these burdens and solve the problem to a certain degree (see https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-datenschutz-anpassungsgesetz-2018.html). The Austrian Amendment Act (österreichisches Anpassungsgesetz) 2018 for the EU GDPR, which is the Austrian equivalent of the German "new BDSG " states that access to personal data could also be limited if an erasure cannot be executed immediately as it is only possible at certain times for economical or technical reasons.

An Austrian legal expert argued that personal data in backups will, depending on the backup concept "outgrow" the backups and will therefore "automatically" become unavailable after a certain "backup period".

Emphasis on Proportionality in the new BDSG

A similarly pragmatic approach can be found within the new BDSG, in § 58 (*Rights to Correction and Erasure and Restriction of Processing*, article 1) to be precise. This section states that instead of erasure, "restricted" processing can be an alternative if erasure is not possible or only possible under "disproportionate effort", a clear hint to the fact that erasure is a rather "flexible" term.

Therefore in accordance with the EU GDPR, a "normal" erasure of personal data can be defined as any process that ensures that the data can no longer be viewed, searched and therefore accessed. Which was, by the way, also the case within the "old" BDSG.

No Specification within the EU GDPR

As a matter of fact, the EU GDPR does not specify this kind of processes or conflicts, for example, by defining the term "erasure", and therefore leaves much room for speculations and interpretations. Only the future jurisdiction will (hopefully) show how to interpret this conflict exactly.

The Erasure Process

Based on the previous argumentation and discussion the process of erasing personal data should be as follows:

1. Initial situation: An affected person demands the erasure of his or her personal data.
2. The demand is registered, documented and forwarded to the responsible person by the data protection officer.
3. The responsible persons within the company check whether the demand is lawful or if other current laws are opposing a possible erasure.
4. If the result of this check is that the requested erasure is lawful, the erasure is executed and logged. If the result of check should show any signs of the request being unlawful, no erasure will be executed.
5. The affected person is informed about the erasure by the company's data protection officer or the responsible person. If the erasure has been classified as being unlawful, the affected person is informed that the erasure cannot be executed due to a conflict with another legislation.
6. The company's data protection officer archives the erasure log in a folder only he or she can access to be able to prove the erasure process at a later point of time within the scope of the documentation obligation.

Right to Object, Data Protection Impact Assessment and Transparency

In general, all documents that are relevant in the context of the EU GDPR can be created and managed with all advantages of an ECM system: may it be a rights concept, a document history, versioning or indexing for quicker retrieval of information or even life cycle settings for automated or manual data erasure, it is all available with windream.

However, there are three other aspects that should be mentioned in that context.

Right to Object

According to article 21, the affected person (data subject) shall have the right to object the storage of their personal data especially according to section (2) which refers to direct advertising. Objections made by affected persons need to be logged and, for example, by using respective access rights, be stored in a protected folder of the ECM system. The same is also true for detected data protection violations, which possibly need to be reported, and for statements of affected persons.

Data Protection Impact Assessment

The same obligation is also valid for data protection impact assessments according to article 35; they also need to be documented in written form. Impact assessments are always necessary before introducing new technologies, for example before installing a new video surveillance system, before introducing a new software, which processes personal data or – a classical scenario – the introduction of a new CRM or ERP system.

Transparency Obligation

And, last not least, the transparency obligation according to article 12 (1) needs to be complied with. According to that article, information about stored data needs to be communicated "in a concise, transparent, intelligible and easily accessible form, using clear and plain language", to quote from the EU GDPR. That topic should also be kept in mind when documenting data protection-relevant aspects.

Further Legal Notes

No Legal Advice by windream GmbH

windream GmbH as a software manufacturer is not authorized to give legal advice of any kind. Therefore, the information contained in this document do not have advisory character. The interpretations of terms and single articles of the EU GDPR are not legally binding information but only reflect opinions regarding and interpretations of the EU GDPR from the point of view of windream GmbH.

Adjustment to National Legislation

The EU GDPR, by means of its flexibility clauses, explicitly intends for the regulations to be adjusted to national legislation by the respective national governments (in Germany the *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU* dated June 30, 2017).

Special Regulations for Processing Special Personal Data Categories

For companies processing special categories of personal data (for example banks, hospitals etc.) special legal categories are valid. Especially when it comes to erasing information from data carriers, these business sectors have requirements which can go beyond the requirements of the EU GDPR (for example multiple overwriting with random data).

Additional Links

The original text of the EU GDPR is available under the following link: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462345886854&uri=OJ:JOL_2016_119_R_0001

The text of the BDSG as adjusted to the EU GDPR (*BDSG-neu* or *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU* dated June 30, 2017) can be downloaded as a PDF file under the following link: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Neues-Bundesdatenschutzgesetz/BDSG-neu.pdf

For interested parties in Austria, the Austrian Chamber of Commerce offers detailed information on the EU GDPR under the following link: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung.html.

Conclusion: Efficient Implementation of the EU GDPR with windream

The above-mentioned aspects of the EU GDPR clearly show that a systematic, consistent, sustainable, compliant and user-convenient implementation of the EU GDPR can only be achieved by using a software tool that fulfills all these requests. Out of all available systems on the market, the ones that are relentlessly focused on the management of information need to be especially highlighted – these are Enterprise Content Management systems such as windream.

Companies that took data protection as seriously as demanded by legal institutions should not have anything to fear, even with the higher sanctions compared to those intended by the BDSG. Nevertheless, it is necessary to assess the data protection practices used in companies and to adjust and refine the data protection management measures to the new requirements of the EU GDPR until May 25, 2018. For that, there is no sample solution, as every company, due to the individual business models, also has individual ways of data processing.

windream as a ”Best Practice“ Solution

The specific implementation of the data protection measures a company needs to fulfil according to the EU GDPR and especially

according to the associated documentation obligations is highly individual. The fact that windream can be used universally, is not limited to certain application areas and can be adjusted to the specific organization structures of a company makes windream a best practice solution for implementing the GDPR requirements.

In this context, once again, the focus is on the complete integration of all ECM functions into the Windows operating system based on a patented software technology. Is there a more efficient way of implementing the legal requirements of the EU GDPR? We don't think so.