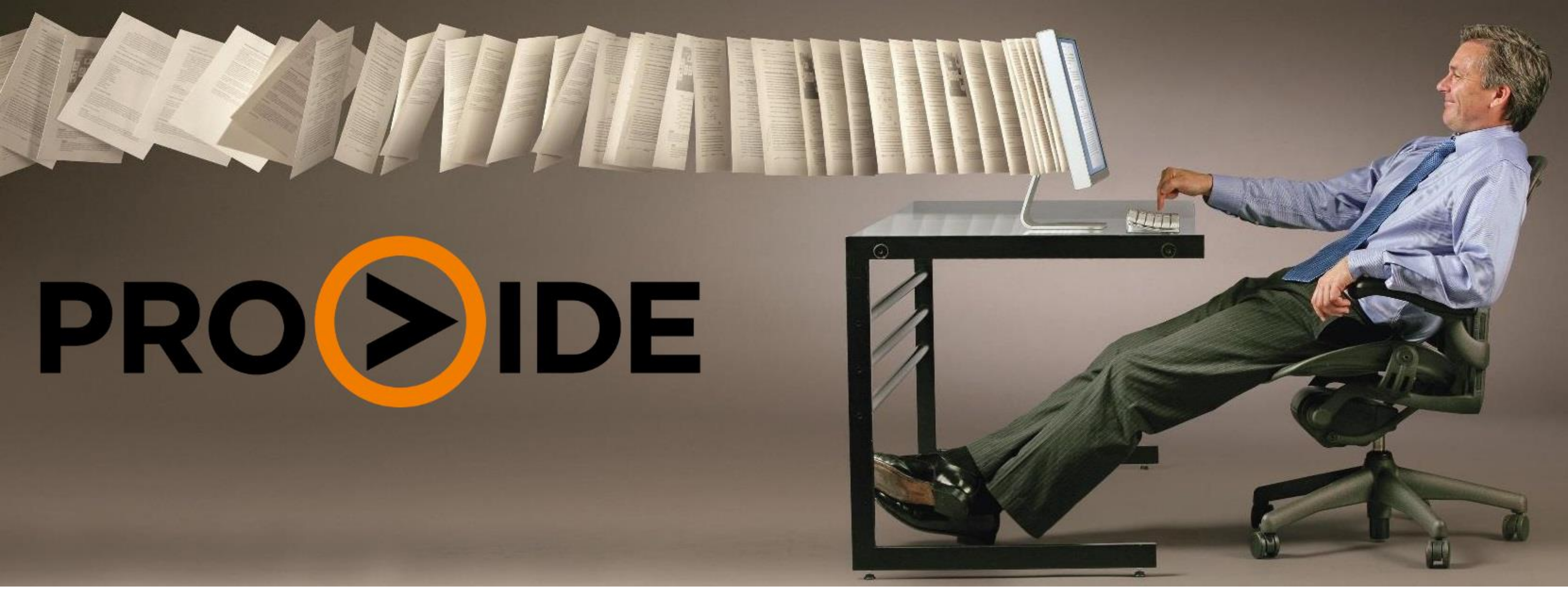

# ProVide vs. GDPR – Thoughts and solutions!

GDPR, the new General Data Protection Regulation that governs the protection of personal data for EU citizens require that organisations secure a legit basis for all manipulation, processing, transfer, distribution and storage of personal data. This applies to both automatic and manual processing. Personal data includes all descriptions, information, pictures and data than can be used to identify a European Union citizen. GDPR demands a clear purpose for data collection, storage and processing and that reasonable technical and organisational measures are implemented to ensure the safekeeping of personal data.

Documentation of all data sources and terms of use, encrypted transfers, and rule enforcement by centralizing data storage are ways to fulfil some of the requirements. The GDPR also imposes principal requirements for adequate and secure (article 32) technical solutions implementing security by design and security by default.

"... Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing." (Legislative act 39)

For management of employee data including, employment contracts, salary information or other information pertaining to an individual, ProVide offers secure and encrypted means to both access, and distribute sensitive data in accordance to the GDPR requirements. Access using the built in user directory, the organisations Active-directory or via direct integration with ERP-systems or other systems offer complete flexibility. Introducing ProVide offers project baseline for succeeding with the mapping and documentation of relevant data sources in preparing for GDPR compliance.

GDPR compliance involves technical as well as organizational processes and routines, legal considerations, and contracts, and in part affects how the organisation is run. By using the technical capabilities of ProVide to centralize, integrate and document ProVide can act as a cohesive force for accomplishing GDPR compliance. Most importantly, ProVide offers a secure, easy-to-use, and cost effective platform for team cooperation and for the distribution/acquisition of data, files and documents in or between organisations.

This whitepaper offers guidance to some of the technical aspects of GDPR and furthermore discusses the support offered by ProVide.

## ProVide as a toolbox

ProVide is a secure and easy-to-use platform for distributing and acquisition of documents and files supporting collaboration between co-workers and internal/external teams. Systematically implementing ProVide offers a route for both directly and indirectly map and solve some of the technical issues and thus moving forward in complying with the purpose and principles of the GDPR.

Introducing ProVide to your organisation offers the opportunity to document and map data sources and the whereabouts of information assets as well as centralizing storage. The technical capabilities of ProVide well exceeds the GDPR requirements of security by design and security by default as it provides secure, encrypted access, that can be properly logged.

- By integrating ProVide to the user management and authorisation system, be it the built in user registry, Active Directory, or ERP-system, employees may e.g. acquire salary specifications directly from ProVide. Mailing salary specifications, as pdf-files, via unencrypted e-mail will most likely not comply with GDPR based on for instance unsecure protocols and redundant storage.
- Access to data and data accuracy. Registered subjects have the right to access all data that have been stored specifically regarding personal data, descriptions and pictures in a reasonable period. Furthermore, subjects also have the right to have erroneous data corrected without unduly delay. ProVide supports implementation of automated scripts, allowing data from mapped sources to be collated, consolidated and presented for access and correction purposes. This empowers the organisation with both data portability and with effective ways to enhance data quality.
- Data minimisation and minimal processing. Only data, relevant for the specific purpose for which it is acquired, may be stored and processed given that the purpose is lawful. Introducing ProVide offers an opportunity to centralize mapping of data, and thereby

establish high quality documentation of relevant data sources. This empowers the organisation to minimise storage, reduce redundancy and eradicate erroneous data.
- The right to be forgotten. Introducing ProVide and thus mapping and documenting data sources establishes a clear depiction of what data need to be deleted or corrected from files, ERP-systems and other sources. GDPR at the very core, requires you keep track of what is stored and where so getting started is of the essence.
- Right to notification if data is compromised. If a security breach compromises personal data, subjects has the right to be informed within 72 hour upon detection. ProVide employs extensive logging capabilities and proactive scripts that, combined with state-of-the-art security design and an array of security mechanisms allows ProVide to detect, log, and implement corrective measures (like blocking access), while directly notifying responsible technicians.

## What does GDPR mean for me?

The General Data Protection Regulation empowers EU-citizens with a strong ownership of their personal data. Companies and organizations may "borrow" and must take care in storing and processing that data for specific purposes rather than owning the data. Contrary to what some believe, the general principle is not to impose constraints to business or hinder the free flow of information. However, the GDPR does force organisations that process personal data to be clear on the purpose and to be meticulous to ensure that the data is processed, stored, and managed lawfully and secured against exposure. It is no longer legit to be sloppy or accept poor IT-security.

## GDPR Principles: What to consider

1. Lawfulness, correctness and openness to provide subjects with the personal information stored. For most organisations using ProVide, lawfulness regarding customer, employee, or other personal data, such as name and contact information may be stored if it relates to a business contract or the intention of signing such a contract. Collecting contact information following consent or for marketing purposes is allowed as long as its purpose is documented.
2. Purpose limitation: Personal data must, not be collected for general purposes, but rather for defined purposes. Member State law or collective agreements, including 'works agreements' (legislative act 155), contracts or intended contracts (legislative act 47, article 6 section 1b) and information for marketing purposes (70) are lawful. Furthermore information related to maintaining security and mitigating fraud

(legislative act 49, 57) may be managed and processed if it complies with GDRP principles, has a defined and at the time valid purpose (article 4, definitions, section 24).

3. Data minimisation. Collected personal data, stored and processed, must be adequate, relevant and limited to what is necessary in relation to the stated purpose. (article 5, section 1c). ProVide in itself minimises data. If you choose to activate auto update or update manually, ProVide will retrieve the update but other than that ProVide sends no information and Västgöta-Data AB has no access whatsoever.
4. Data accuracy. Personal information shall be correct and updated without unduly delay. Accuracy is a key concept in that accuracy also entails trust. Is everyone working on the latest version of a document or blueprint? Did I get the latest version via mail and did it come from the proper source? Using ProVide server secures trust that all information, documents and blueprints come from a central trusted source and that all parties get the latest version. Whether you are providing salary specifications to your employees or teaming up with consultants on the latest architectural blueprint in a shared document space, accuracy and trust is key!
5. Storage limitation. Storage of personal data, in which subjects can be identified, is allowed only within the period required to fulfil the purpose for which the data was collected. Data collection, processing and storage must be lawful and safeguarded by technical and organisational measures. Data may also be stored for longer periods e.g. for statistical, historical or even other purposes if identifiers are removed or. ProVide offers powerful scripting features both internal and external that may block access to old data as well as executing events, notifying staff or even for scrubbing data.
6. Integrity and confidentiality: Requirements for technical solutions relative to the processing of personal data should involve risk assessment based on the sensitivity of the data, the magnitude of the processing and the purpose for which it is being processed (legislative act 76). The principles of security by design and security by default (legislative act78, article 25) further stresses that reasonable data security is not an option but a requirement. ProVide allows login and access procedures governed by central user management and authorisation systems. This reduces risk for both administrative errors and for privilege escalation. Security levels are adjustable depending on your preferred set of encryption protocols. Enterprise level certificate support furthermore enables verification of server identity.
7. Accountability. The data controller must be able to demonstrate compliance to the points above and particularly to number one. Introducing ProVide enables proper access, event logging as well as supporting, data centralisation, -mapping and -integration.

To summarize. GDPR requires organisations to keep track of what personal data is stored, where it is located, the lawful purpose for which it was collected, and when and how to delete it. Technical and organisational IT-security considerations are mandatory.

# ProVide is developed by Västgöta-Data AB

For more than a decade, ProVide has been an easy-to-use, secure and flexible file sharing software. The software targets teams and co-workers that need to securely cooperate on large or small documents and files. The administrative interface is in English, whereas end users and partners can access and collaborate on files, folders and documents in several world languages including; Mandarin (simplified, PLC), Chinese (traditional, Taiwan), German, French, Spanish, Japanese, Thai, Turkish and English. Globally, ProVide currently has more than 4000 customers in Banking, FinTech, Governmental & Municipal organisations, Defence Industry, Universities, Telecom as well as customers in other industry- and service sectors.

The addition of GDPR as well as recent events in western media concerning security breaches, and the massive lawful and unlawful spreading of personal data stressed many of the concerns that the legislation targets since its introduction on the 27th of April 2016. ProVide is THE affordable, easy-to-use and secure productivity enabler for organisations that want secure access to shared files and folders across teams or to co-workers. ProVide benefits any organisation that must not, should not, or should think again, before using Dropbox, Google Drive or WeTransfer to transfer and track of sensitive business data. ProVide keeps information access strictly under the control of designated users and the organisation.

VÄST
GÖTA
DATA

Västgöta-Data AB offers both the ProVide MFT server software as well as services in digitalization, software development and integration and consultancy services. ProVide is available globally as a license subscription service along with optional SLAs along for support, integration and custom development services. Our support department specializes in highly automated support using remote monitoring and management software. The company primarily targets SMEs although several Fortune 500 companies also adopt ProVide.

Everything we do, from offering support, to developing and integrating software solutions has one focus: To manage the secure flow of business critical data that can be trusted for privacy, correctness and availability using excellent software and tools.

Phone: +46 500-44 89 97
support@provideserver.com
https://www.vastgotadata.se
https://www.provideserver.com

*This white paper does not constitute legal advice but gives a brief walkthrough of GDPR.
For reference to the legislative text, please follow the link to the PDF below:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1