TIA and the EU General Data Protection Regulation (GDPR)

White Paper

September 29, 2017 – note that content is subject to change

TIA® Closer to Customers

TIA Technology A/S
Bredevej 2
DK-2830 Virum
Denmark
T +45 7022 7620
F +45 7022 7621
W tiatechnology.com
E marketing@tia.dk

Contents

Introduction

EU legislation on data protection has been in place since 1995. However, with the rapidly growing and constantly changing digital landscape, processing of personal data has grown exponentially and the rules needed modernizing. Also, the implementation of data protection laws in different countries needed to be consistent.

With this as a background, EU adopted the data protection reform package in April 2016. The package includes the General Data Protection Regulation ("Regulation") which governs privacy rights, and the Data Protection Directive for the police and criminal justice sector.

Generally, the reform changes give people more control and transparency over their personal data and better protection of privacy. The new rules impact solutions that store personal data, like TIA. Regulation highlights are that

- Right to have personal information deleted when no legitimate grounds exist to retain it.
- Protection of personal data must be part of solution design.
- Each individual must have easier access to their own data.
- Companies are to obtain consent from individuals when personal data is collected.
- Individuals have a right to suspend handling of their personal data.
- Individuals have a right to know if their data has been compromised; companies have a duty to inform the individuals and authorities in case of a breach.

This White Paper briefly outlines the key requirements in the regulation and then discusses how the requirements will be implemented and supported in the TIA Solution.

The support to ensure compliance is delivered as a packaged solution called TIA GPDR[1] Compliance Package. The package is a combination of amendments to the TIA Solution and configuration and implementation updates. The GPDR compliance package functionality is delivered with TIA 7.5.1 and TIA 6.4.4.

The full TIA GPDR Compliance Package includes consultancy and implementation to ensure compliance with the Regulation. The offering includes implementation and configuration as well as advice on roadmap and handling of data in associated solutions. Engaging with TIA Services & Solutions will include:

- Presenting a plan for custom implementation
- Ensuring that any customized information, for example captured in flexfields, are included in scope
- Installing the solution at the customer site and working with onsite QA to validate the updated solution.

All EU Member States have to comply with the directive by May 25, 2018. Companies operating in EU must comply at the same date. Failing to comply may be heavily fined: depending on the severity of the offense the fines may be up to 10 million euro

[1] **G**eneral **D**ata **P**rotection **R**egulation

or 2% of the total global annual turnover/GWP or up to 20 million euro or 4% of the total global annual turnover/GWP.

Need more information?

TIA White Papers – TIA Technology has created several industry-relevant White Papers that can be downloaded from: www.tiatechnology.com

You are always welcome to contact TIA Technology at tia@tia.dk.

Regulation requirements

On April 14, 2016 EU passed the new regulation for handling and protection of person-related data. The regulation enters into force in all EU member states on May 25, 2018.

Two-thirds of Europeans are concerned about not having complete control over the information they provide. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed. The Regulation strengthens the right to data protection, and enables Europeans to have trust when they give their personal data.
The purpose of the **General Data Protection Regulation** (GDPR) is to enable individuals to better control their personal data. Two-thirds of Europeans are concerned about not having complete control over the information they provide. Seven Europeans out of ten worry about the potential use that companies may make of the information disclosed. The GDPR strengthens the right to data protection, and enables Europeans to have trust when they give their personal data.

Strengthening citizens' rights and empowering individuals

The Regulation gives individuals more control over their personal data and focus on:

- **Data protection by design and by default**: "Data protection by design" and "Data protection by default" are essential elements in EU data protection rules. Data protection safeguards must be built into products and services from the earliest stage of development, and privacy-friendly default settings will be the norm.
- **The right to know when one's data has been hacked**: Companies and organizations must notify the national supervisory authority of data breaches which put individuals at risk and communicate to individuals all high risk breaches as soon as possible so that users can take appropriate measures. **Easier access to one's data**: Individuals will have right to obtain information on how their data is processed and this information should be available in a clear and understandable way. A **right to data portability** will make it easier for individuals to transmit personal data between service providers. Storage and processing of data requires the individual's **consent** or that the processing is needed to perform a contract, which the individual has entered into or required by law.
- **A "right to be forgotten"**: When an individual no longer wants her or his data to be processed, and provided that there are no legitimate grounds for retaining it, the personal data must be delete. Individuals can also request that wrong data is deleted.
- **Stronger enforcement of the rules**: Data protection authorities will be able to fine companies that do not comply with EU rules up to 4% of their global annual turnover.

Right to be forgotten: How will it work?

Already the current directive gives individuals a possibility to have their data deleted, in particular when the data is no longer necessary.

For example, if an individual has given her or his consent to processing for a specific purpose, like display on a social networking site, and does not want this service anymore, then there is no reason to keep the data in the system.

This does not mean that on each request from an individual all his personal data are to be deleted at once and forever. If for example, the retention of the data is necessary for the performance of a contract or for compliance with a legal obligation, the data can be kept as long as necessary for that purpose.

The provisions on the "right to be forgotten" are very clear: freedom of expression, as well as historical and scientific research are safeguarded. For example, no politician will be able to have their earlier remarks deleted from the web. Amongst other things, this means that websites will continue operating on the basis of the same principles.

References

Below list of references were used when this document was created.

• Reform of EU data protection rules	The EU data protection summary page; this page is regularly updated.
• Regulation (EU) 2016/679	Actual General Data Protection Regulation text.
• European Commission – Press release	EU press release from December 2015 about the two instruments of the Reform: • The General Data Protection Regulation and • The Data Protection Directive.
• General Data Protection Regulation	Wikipedia background article.
• Top 10 operational impacts of the GDPR: Part 3 – consent	The third article in a series of articles addressing the top 10 operational impacts of the GDPR, from January 2016. The article links to the previous two articles.
• GDPR in Danish companies	Confederation of Danish Industry / DI page; the page is in Danish but the implementation guide that the page links to is available in Danish as well as in English.

TIA Solution and the GDPR

The Regulation introduces a number of requirements which all insurers need to address:

- The right to be forgotten.
- Data protection by design and by default.
- The right to suspend data handling.
- Duty to inform individuals and authorities if data has been compromised (incident handling/notification).
- Easier access to one's data.
- The right to data portability.

These requirements and the way they are handled in TIA are discussed below. The described new functionality is introduced to TIA in TIA 7.5.1 and TIA 6.4.4. The right to use the new functionality is obtained through a separate contract with TIA Technology.

Right to be forgotten

During the course of a normal workday, insurers collect and store personal data for a variety of reasons. Insurers are obliged to get consent from a prospective customer for any data collection and data storage. Using this data is justified while the insurer has a business relation with the individual, but what do insurers do when this relation no longer exists or if the data collected is incorrect?

The GDPR package includes functionality, which ensures that all personal data can be cleaned up from the system, when a business relationship expires. TIA's clean-up function offers "house-keeping" to ensure that data eligible for deletion based on age is removed from a production environment.

The GDPR package supports these insurer needs:

- The need to comply with regulations concerning handling of personal data. Transient information, for example data used for quotes or for parties created on self-service web sites, can typically just be deleted.
- The need to periodically trim the data database for obsolete data; removing data frees up space and also has a positive effect on system performance.

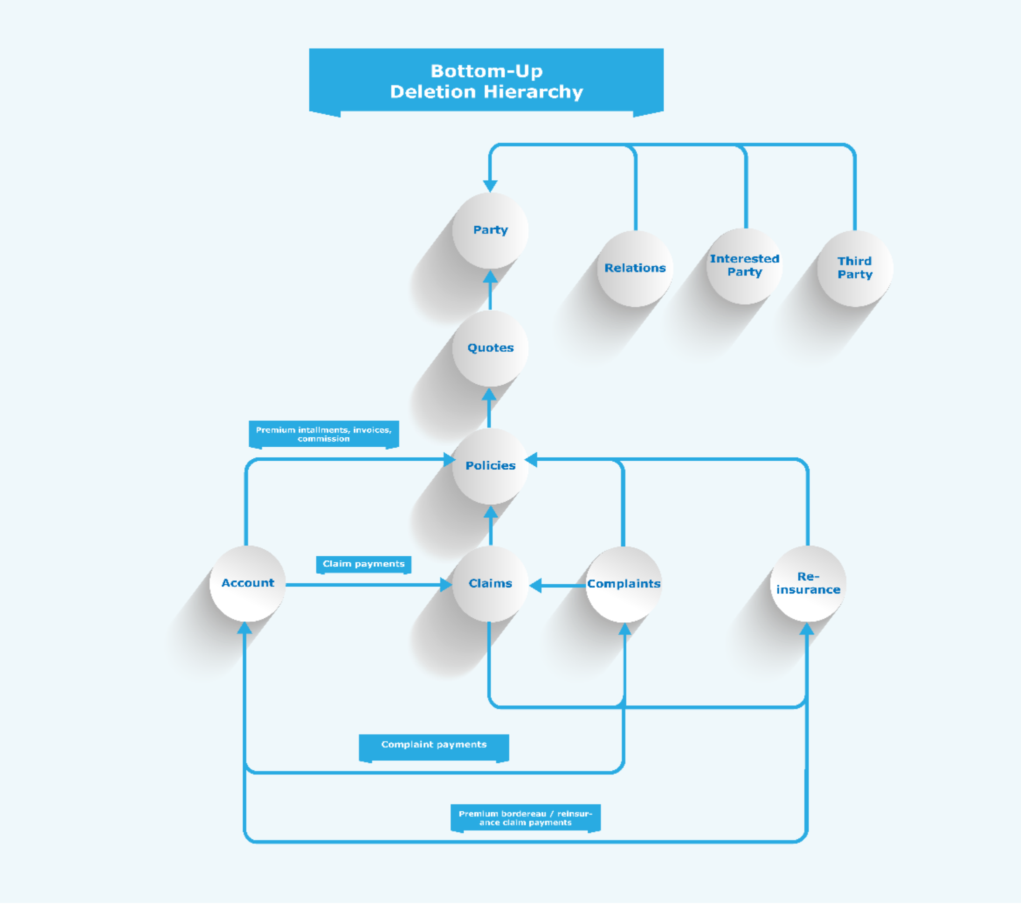
The package consists of a set of programs to clean up personal and obsolete data stored in different TIA modules. Processing will be based on a set of rules, which are defined and configured on site. The rules can be based on business relationships and can be set up by business users, for example compliance officers, which makes the solution flexible and adjustable. For example, rules might specify that customers with no claims and no polices are deleted after 30 days, customers with personal injury claims are stored for 30 years but polices and claims not related to the peronal ingury are deleted sooner.

The automated processing is supplemented with a manual option: users can delete data manually through the TIA UI by providing exact instances (party number or policy numer) to be deleted. This could for example be relevant in instances where existing data is found to be wrong.

The GDPR package also includes clean-up of old transactional data in single, high volume static database tables. Configuration options ensure that the storage period is long enough to satisfy specific company needs. Manual deletions and the automated process follow same validation rules.

Stringent system validations ensure that data integrity is maintained at all time in case of data deletion.

The diagram below illustrates functional dependencies in the main TIA modules where personal data is stored. When obsolete data is deleted, the process starts at the bottom and continues upwards.



For example, account data is deleted first, starting from the bottom. If account data is deleted successfully then further entities, like claims, can be processed. Policies can be erased when all related claims and financial data have been deleted. As a last step, party entity and all related information is cleaned. This mechnism ensures that qoutes (without claims and account transactions) are handled after a shoter period than polices and claims.

Data protection by design and by default

The TIA Solution already includes authorization and access settings which can be used to ensure that personally identifiable information or sensitive personal information can be seen only by the appropriate insurance company employees.

TIA Solution enforces role-based access to sensitive data. TIA authorization settings enable insurers to define the users or user groups who can view and edit data.

The authorization settings control access to the following data:

- **Party data**: Data identifying a customer is not considered sensitive, hence no restriction is added to party data
- **Policy related information**: Access can be limited to specific clauses and coverages for a given policy. Many person insurances hold sensitive data on the "description of the insured object", for example a person. Consequently, TIA access control is on the insured object level.
- **Financial transactions**: Payment instructions and general payment information is not to include sensitive data hence TIA is enforcing restrictions to financial/account information
- **Claims data and history**: TIA authorisation mechanism controls access to specific types of claims. Handlers without authorisation can see that a claim exists but not the content; only authorised handlers can see and work on personal injury claims.
- **Communication and documents**: TIA ensures that communications and documents, including images, are subject to the rules of the related entity, for example claims or policies.

The solution supports a granular security access, as shown in an example below:

Level 1	Security level 1: All claim handlers have this level as a minimum. Allows the user to handle all standard property
Level 2	Security Level 2: Allows the user to also handle auto claims
Level 3	Security Level 3: Allows the user to also handle commercial claims
Level 4	Security Level 4: Allows the user to also handle casualty claims
Level 5	Security Level 5: Allows the user to also handle workers' compensation claims

Note that by default users have no access: all users need to be assigned a security level to access data.

Right to suspend data handling

In situations when a dispute exits between an insurance data handler and an individual regarding the insurer's right to process the individual's data, manual data processing can be temporarily suspended for a specific individual.

Insurers manage temporary suspension using an option on the party object. When enabled, all data related to the party are in "read-only" mode and no data can be changed by a user. Underlying processes continue and premium is still collected.

The right to know when one's data has been hacked

A breach in data security needs to be identified and needs to trigger the appropriate actions, depending on the severity.

Current TIA version reduces the risk of a breach by automatically enforcing timeout in the front-end.

Any data modification in TIA is logged with a user id and a time stamp. This makes it possible to document who changed or entered data and an audit trail is in place in case of an incident resulting in data changes. This audit mechanism is extended with logging on all login to TIA and all login attempts.

TIA GDPR package enables logging of viewed data, which support the documentation of the impact of a possible breach. The package provides relevant context information (including IP-address) for Oracle Audit. Oracle Audit can be activated for logging of user activities. TIA provides guidelines and sample configuration tracking to follow session and thereby help identify compromising actions and who has been compromised.

Easier access to one's data & Right to data portability

TIA GDPR Package supports both requirements with one standard solution. The philosophy is to provide a dynamic output API and implementation guidelines, which will enable and speedup the introduction of new customer facing communication like new portal sites or standard documents.
The new dynamic output API solution enables insurance companies to configure an unlimited number of RESTful APIs, that will return a response in JSON format to be used in preferred communication channels with customers e.g. customer portals, output solutions etc.

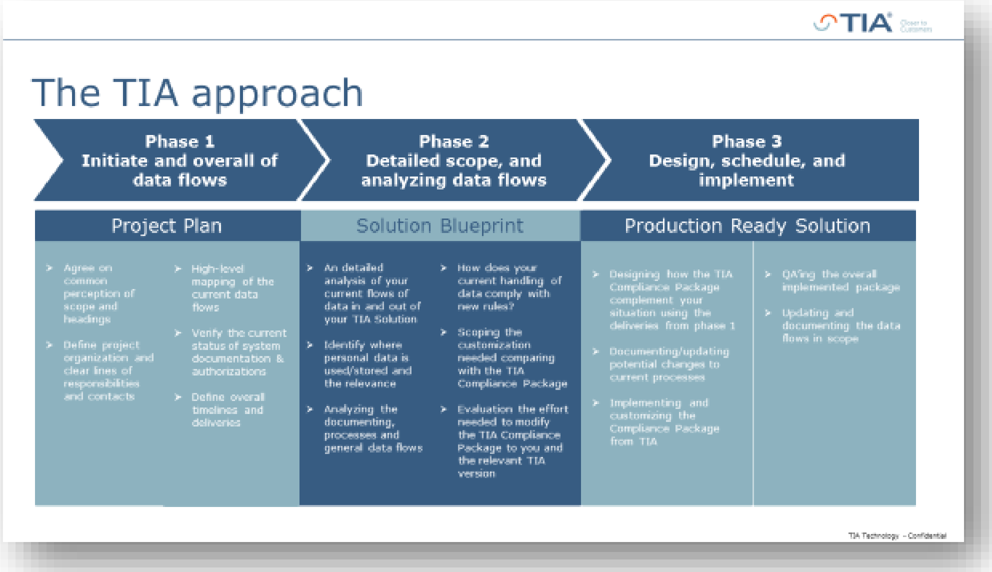
The flexible solution will give freedom to insurance companies to interpret themselves, what is own data and what data is needed in portability situations. TIA will provide examples for inspiration. The solution will support variations in customers, insurance products, etc. and no separate deployments needed, when APIs are updated as everything is 100% configured.

Implementation considerations

General considerations

TIA Services & Solutions has built up substantial know-how within taking a standard deliverable to customers and ensuring that the final solution caters for the customer specific needs. TIA Services & Solutions' offering provides a solid plan of action and best practices on the solutions supporting the EU Data Protection regulation.

When engaging with consultants from TIA Services & Solutions, a joint effort will identify custom code which need to be included and potential extensions and custom forms. For the partner and the customer this means certainty of full compliance and a working solution which is up and running with a minimum of pull on internal resources. The service will be provided with the following themes in focus:



The TIA approach

Phase 1
Initiate and overall of data flows

Phase 2
Detailed scope, and analyzing data flows

Phase 3
Design, schedule, and implement

Project Plan

- Agree on common perception of scope and headings
- Define project organization and clear lines of responsibilities and contacts
- High-level mapping of the current data flows
- Verify the current status of system documentation & authorizations
- Define overall timelines and deliveries

Solution Blueprint

- An detailed analysis of your current flows of data in and out of your TIA Solution
- Identify where personal data is used/stored and the relevance
- Analyzing the documenting, processes and general data flows
- How does your current handling of data comply with new rules?
- Scoping the customization needed comparing with the TIA Compliance Package
- Evaluation the effort needed to modify the TIA Compliance Package to you and the relevant TIA version

Production Ready Solution

- Designing how the TIA Compliance Package complement your situation using the deliveries from phase 1
- Documenting/updating potential changes to current processes
- Implementing and customizing the Compliance Package from TIA
- QA'ing the overall implemented package
- Updating and documenting the data flows in scope

TIA Technology – Confidential

Right to be forgotten

The TIA GDPR Package handles data stored in the standard TIA Solution. For custom solution implementation, which TIA Services & Solutions can assist with, it must be considered whether some insurance company data is outside of the TIA solution and related to the data to be deleted. Insurance companies must consider:

- Defining additional retention rules
- Customization within the TIA solution
- Surrounding solutions like Data Warehouse (DWH), Document Management Systems, and CRM

The TIA GDPR Package provides tools which makes it possible to trigger deletion of dependant data in non-TIA Solution sources. TIA Technology can help set up specific rules and integrations to other solutions to trigger data deletion.

Data protection by design and by default

The solution is utilizing the existing authorisation functionality within TIA, hence implementation will require that you revisit configuration of roles, profiles and authorisations as well as configuration of "sensitive data'. TIA Services & Solutions assists you in categorising data and ensure the appropriate protection.

The right to know when one's data has been hacked

The support for this requirement is covered by a number of initiative, for example defining an incident, plan of actions for the incidents. TIA Services & Solutions assists with best practice on tracking or audit of queried data[2] as well as configuring handling of incidents and automatic identification or privation of incidents.

Easier access to one's data and the right to data portability

TIA is delivering a generic Application Programming Interface (API), which is to be tailored to local requirement and application landscape. Any local communication platform must be amended with handling of customers requesting and delivering information, for example, a customer portal needs a "your own data page".
The content of the APIs are to be configured in TIA configuration area based on the local definition of own data. TIA offers support for the API and can help develop or tailor APIs optimized for local requirements.

Right to suspend data handling

The solution will not require configuration; the only implementation effort considered is a porting to your TIA version.

[2] Utilzing Oracle standard tools: https://www.oracle.com/database/security/audit-vault-database-firewall/index.html

Summary

Below table list the requirements discussed in this White Paper and summarizes the suggested solution for each.

Requirement	**Solution**	**Implementation**
The right to be forgotten	Delete data based on a predefined rules set.	Configure handling rules and address data in the entire IT landscape, GDPR extension.
Data protection by design and by default	New authorisations on data access e.g. authorisation on claim with a specific class or specific party data.	Revisit configuration of roles and authorisations.
The right to suspend data handling	Enable a lock on manual handling.	Grant lock authorisation to relevant person/role, for example Data Protection Officer.
The right to know when one's data has been hacked	Utilize existing security and add additional logging to ensure audit trail in case of breach.	Best practices on processes, configuration of role and responsibilities. Technical support of audit on queries.
Easier access to one's data and data portability	Standard API for integration to customer portals, output solutions etc.	Evaluate data set in API and implement the communication channels e.g. portal site, report etc.

Timeline

TIA GDPR compliance package was released with TIA 7.5.1 in August, 2017 and with TIA 6.4.4 in September, 2017.

TIA Technology is currently engaging with authorities, legal advisors, customers and participation in knowledge groups in different interest organisations to ensure that TIA incorporates the adjustment that might appear to the implementations of the regulations.

Simultaneously TIA Services & Solution have prepared an offering of services, which will ensure that you follow a structured and efficient process toward compliance. The process is following best-practice compliance processes proposed by legal advisors. The services include analysing IT and data landscape, plan the roll-out of adjustments etc. We recommend that you start the analyses and planning as soon as possible to ensure that you are compliant by May, 2018that you are ready to receive the TIA GDPR compliance package is August, 2017. Please engage with you TIA account manager to build a specific plan for you.

FAQ

Will the solution be ready for my version of TIA? TIA GDPR package is released with and build for TIA 6.4.4 and TIA 7.5.1 (Forms and ADF). TIA implementation services can include an upgrade to the newest TIA version or enabling the functionality for a specific customer implementation. This is subject to a separate service agreement.

What about my custom Forms?
By engaging with TIA Services & Solutions you will be able to get a customized implementation embedding your own developed code.

How do I get audit on queried/ viewed data? Our interpretation is that regulation is not enforcing a log on all queried data as we are ensuring that only authorised persons can access data. However, this is an interpretation based on general dialogues with legal advisors at customers and authorises. Local interpretations could impose full audit on viewed data. This can be activated with Oracle Audit[1]. Oracle Audit enables setting up a logging mechanism in order to track and document who has accessed which data in the TIA solution. TIA will deliver at standard configuration and a cookbook for activation of Oracle Audit[3]. TIA Services & Solution is able to support you in the analysis and do the actual implementation of Oracle Audit.

Will anonymization or encryption of data be sufficient for "the right to be forgotten"?
This is an ongoing discussion in the GDPR communities and varies from country to country. The essence is that you do not comply with GDPR if you can restore data or if you in anyway can link/trace data to a person. The right to be forgotten talks explicitly about deletion. TIA need to keep policy id, Party id etc. to keep the database integrity. Those identifiers could potentially identify a person. Especially if correlated with other data. The will result in a breach with GDPR. Hence deletion is the only certain solution for the requirement.

The Regulation promotes techniques such as anonymisation, pseudonymisation, and encryption to protect personal data in relation to "Data protection by design and by default" within "big data" analytics.[4] TIA BI cloud will therefore ensure that data is anonymised.

What is the commercial impact? TIA GDPR compliance package is introducing new functionality. The right to use the new functionality is subject to separate contract. Oracle Audit is a separate Oracle solution with separate licence (see above). TIA Services & Solutions offerings are consultancy services following TIA consultancy rates.

[3] https://www.oracle.com/database/security/audit-vault-database-firewall/index.html
[4] http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

When should I start my compliance implementation? Now. TIA recommends that you start TIA analysis phase 1 (see above) ASAP.

What's next? TIA Customer Services will contact you to start the planning the process during 2017. If you have further questions, please feel free to contact you TIA Key Account Manager or TIA Customer Service at tia@tia.dk need more information.

Head office

Denmark

TIA Technology A/S
Bredevej 2
DK-2830 Virum
Denmark

Phone: +45 7022 7620
Fax: +45 7022 7621

tia@tia.dk
www.tiatechnology.com

Offices

Germany:
+49 711 222 54 490

Lithuania:
+370 626 50655

Poland:
+48 22 5286673

South Africa:
+27 (0) 11 258-8533

This document may not be reproduced or transmitted in any form or by any means, for any purpose, without prior written approval of TIA Technology A/S. The contents of this document are continually subject to amendment without prior notice. Although due care and diligence has been taken to ensure accuracy of this document, TIA Technology A/S does not undertake any liability for the accuracy of the document, including errors and omissions.

This document shall not impose any obligations on TIA Technology A/S by any means.