Duck Creek
Technologies

General Data Protection Regulation

A GUIDE TO THE EUROPEAN UNION GDPR

Executive Summary

Insurance providers are preparing for new E.U. regulatory requirements that are due to take effect in May of 2018 under the General Data Protection Regulation (GDPR). The purpose of this regulation is to protect E.U. residents' personal data as they engage in online activity and transactions. This Duck Creek guide analyses select provisions of the GDPR to provide additional information to our customers who are subject to these regulations. It includes excerpts from relevant sections of the GDPR itself, suggests considerations for GDPR implementation, and includes links to feature descriptions and guidance produced by Duck Creek technology partners. In support of this guide to the GDPR, Duck Creek has produced a Personal Data Inventory to help our customers identify and classify personal data in support of their GDPR compliance obligations.

Supporting Data Privacy Compliance

Duck Creek supports insurance providers around the globe who are subject to specific local regulatory requirements. As measures like the GDPR evolve and regulatory bodies establish enforcement track records (e.g. the Article 29 Working Party; the U.K. ICO), Duck Creek monitors these sources, as well as industry publications and customer feedback channels, in order to respond to any required changes. We are committed to delivering features and products that provide tools that allow insurance providers to maintain compliance with these important regulations.

To ensure regulatory compliance, insurance providers rely on internal groups and processes to monitor and evaluate regulatory changes, like those required by the GDPR. These groups compile information from industry sources (e.g. this guide) to inform their perspectives on how insurance providers should address regulatory compliance. When required changes are identified, insurance providers can use Duck Creek software to configure required rules, processes, and workflows to achieve regulatory compliance.

Preparing for Data Identification & Classification

As part of the initial implementation of GDPR compliance and as part of subsequent maintenance activities, insurance providers must identify and classify personal data items, the majority of which are used across multiple systems (both Duck Creek and non-Duck-Creek). The resulting catalogue of data items may be consolidated into an enterprise-wide data inventory, which supports the ongoing abilities to:

- Search for and identify personal data
- Facilitate data classification
- Maintain an inventory of personal data holdings

An insurance provider's resulting data inventory provides the basis for supporting each data subject's individual rights, which are key parts of the GDPR data protection principles. In support of an insurance provider's data identification and classification activities, Duck Creek provides a Personal Data Inventory to identify and describe the personal data stored, processed, and transmitted by Duck Creek solutions. Additionally, the new Microsoft Data Discovery & Classification feature, released 15 February 2018, should be considered as a tool to support those efforts. Using one or both tools, insurance providers can maintain an up-to-date inventory of all personal data items, their locations across the enterprise, and any required regulatory classifications. Learn more in the Additional Resources section in the last two pages of this white paper.

GDPR Individual Rights and Company Obligations

The GDPR data protection principles are comprised of a set of individual rights (for data subjects) and a related set of company obligations (for data controllers and processors). This guide covers the following rights and obligations:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- Rights related to automated decision making
- The obligation to provide data protection by design and by default

Each right is reviewed below in terms of how it is characterised within the GDPR itself, and the ways in which our customers can take action using Duck Creek solutions to support each principle.

The right to be informed

The GDPR requires insurance providers to provide:

- "Fair processing information," typically through a privacy notice
- Transparency over how personal data is used

The right to be informed emphasises an insurance provider's obligation to provide a communication mechanism (i.e. a data privacy notice) that clearly describes how it uses a data subject's personal data throughout its enterprise. This privacy notice must clearly explain all processing activities that use personal data and whether those activities are initiated by the insurance provider or its third-party processors. The insurance provider typically provides the privacy notice to the data subject prior to the initiation of processing activities. The Duck Creek Personal Data Inventory and online feature documentation in our Solution Center should be leveraged to contribute to the required detailed processing activity descriptions for each personal data item.

The right of access

The right of access guarantees the data subject may:

- Access their personal data and supplementary information
- Be aware of and verify the lawfulness of the processing

Duck Creek provides a comprehensive set of application pages and system capabilities that facilitate personal data searching, processing, and reporting. In addition to the rich capabilities provided, an insurance provider can use Duck Creek configuration tools to create and expose additional access points, processes, and report options to support the data subject's right of access.

As part of completing the Duck Creek Personal Data Inventory, the insurance provider establishes the lawfulness of the processing by describing the reason the process is required. This legal justification must be available in the customer data privacy notice, for customer inquiries about acceptable use, and for requests to discontinue or suspend processing.

The right to rectification

As the insurance provider collects data about a data subject, the GDPR:

- Ensures individuals are able to have incorrect or incomplete data corrected

Requests for correction or completion of data are processed by an insurance provider on the related Duck Creek application page, by using automated business rules or using Duck Creek Anywhere APIs. The insurance provider can automatically confirm changes with configured business rules or with notification provided to third-party processors through Duck Creek Message Hub integrations.

The right to erasure

The right to erasure requires an insurance provider to locate and erase personal data upon request. This right is also referred to as "the right to be forgotten," and it allows an individual to:

- Request the deletion or removal of personal data where there is no compelling reason for its continued processing

After the insurance provider completes the Personal Data Inventory, the inventory contains locations of all personal data elements, whether located in the Duck Creek application database or in files on the transaction server. The insurance provider uses the locations recorded in the Personal Data Inventory to identify and erase a data subject's personal data, either as part of a configured application page or an automated process. Duck Creek will share any common implementation patterns for those application pages or automated processes on our Content Xchange as they become available. The topic of data masking or anonymisation is discussed below in the Data protection by design and by default section of this white paper.

The right to restrict processing

Data subjects have the right to request that their insurance provider discontinue or restrict any processing that uses their data. This right specifies that:

- Individuals have a right to "block" or suppress processing of personal data
- When processing is restricted, it is permissible to store the personal data, but not to use it for further processing
- Just enough information about the individual can be retained to ensure that the restriction is respected in the future

After an insurance provider completes a Personal Data Inventory, the inventory identifies and describes the baseline capabilities and implementation-specific capabilities for discontinuing and restricting personal data processing. To complement the configuration documentation created by the insurance provider during implementation, Duck Creek provides extensive feature documentation through our online Solution Center, which describes the base-provided capabilities for discontinuing and restricting processing. To record and enforce the process restriction request, Duck Creek applications provide the ability to record contact notes; for example: Policy Notes, Bill Account Notes, and Claims File Notes.

Insurance providers can also use Duck Creek configuration tools to add workflow rules that prevent data processing activities until they receive the data subject's unambiguous, granular consent. For example, insurance providers can use the Duck Creek Author configuration tool to add a rule to quote workflow that prevents a user from processing a quote until the data subject provides their consent.

The right to data portability

An insurance provider is required to provide a data subject with their personal data in a common, structured format, so they may:

- Obtain and reuse personal data for their own purposes across different services
- Move, copy, or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability
- Take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits

Using locations recorded in a Personal Data Inventory, an insurance provider identifies all instances of personal data and presents them on a configured application page, letter, or report. In response to data subjects' requests for their personal data, this data may be provided in any common, easily-understood format. Common formats configured during implementations include a printed form (e.g. Duck Creek Forms) or a built-for-purpose report that renders data as required (e.g. in XML or Excel formats through a reporting solution).

Rights related to automated decision making

Insurance providers must identify decisions or processing performed completely or partially by automated means. Since the insurance provider must disclose (e.g. through a privacy notice) how sensitive data is used, this provision:

- Provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention (including profiling)

In feature documentation on our Solution Center, Duck Creek identifies and describes base-provided processes and the personal data items involved. During implementation, an insurance provider completes a Personal Data Inventory along with feature configuration documentation. When used together, these references provide logical descriptions of how the insurance provider's automated processes use personal data within Duck Creek solutions.

Data protection by design and default

Insurance providers have an obligation to create and maintain enterprise-wide plans to develop technology, products, processes, and organisational structures with data protection and privacy as integral components. The GDPR emphasises that:

- Companies have a general obligation to implement technical and organisational measures to show consideration and integration of data protection into their processing activities

Duck Creek software and its underlying platform technologies provide the tools necessary for insurance providers to comply with data privacy regulations. These may include:

- User permission and authentication capabilities, allowing for a restricted subset of users to access or change personal data (e.g. User Administration)
- Encryption of personal data at rest through volume-level encryption using BitLocker and Microsoft Transparent Data Encryption (TDE) for MS SQL Server or Azure Server (see Infrastructure Security below)
- Use of TLS/SSL and IPsec for in-flight data encryption (see Infrastructure Security below)
- Data masking or obfuscation (e.g. via the Duck Creek Author configuration tool)

Conclusion

Duck Creek customers transact business all over the world and must comply with all applicable regulatory requirements, such as those specified in the GDPR. As a core insurance software provider, Duck Creek has an ongoing commitment to build globally applicable capabilities that enable insurance providers to meet their local regulatory obligations and compliance requirements. To that end, as insurance providers utilise Duck Creek software tools to configure required rules, processes, and workflows, Duck Creek encourages a close relationship with the local London, U.K. team and your dedicated Customer Account Manager for any assistance Duck Creek may offer.

Additional Resources

Duck Creek Personal Data Inventory

Duck Creek provides a Personal Data Inventory to support an insurance provider's efforts to identify, classify, and describe personal data and those system processes which use personal data. The inventory consists of two separate tabs: Identification and Processing.

Identification

Personal data elements provided through the base data model are pre-filled on the Identification tab with their location and description. The insurance provider completes the information type and sensitivity level and adds any new, custom data elements specific to their implementation.

Processing

The Processing tab is pre-filled with the most commonly used base processes, according to their type, category, and description. The insurance provider customises the type, category, and description and adds any new or customised processes specific to their unique implementation.

Microsoft Data Discovery & Classification

Duck Creek recommends evaluating the Microsoft Data Discovery & Classification feature, released 15 February 2018, to support data identification and classification activities.

- For on-premises installations of Duck Creek software, data discovery and classification are available through the customer's use of SQL Server Management Studio
  - https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-data-discovery-and-classification
- For OnDemand, data discovery and classification are available through Azure SQL
  - https://docs.microsoft.com/en-us/azure/sql-database/sql-database-data-discovery-and-classification

Infrastructure Security

Duck Creek maintains a partnership with Microsoft, a key platform technology partner. Microsoft provides several infrastructure security products and features, which are used to enforce data encryption for Duck Creek OnDemand and for on-premises Duck Creek deployments. Those encryption technologies, as they pertain to the GDPR, are covered in detail in Microsoft's Guide to enhancing privacy and addressing GDPR requirements with the Microsoft SQL platform. Microsoft reviews the GDPR and their products provided for GDPR compliance in Beginning your General Data Protection Regulation journey for Windows Server.

Encryption at rest

- For Duck Creek on-premises installations, data at rest is encrypted through the insurance provider's use of SQL Server TDE (transparent data encryption). For Duck Creek OnDemand deployment, data at rest is encrypted by default on OnDemand servers through Azure SQL TDE (transparent data encryption)
  - http://msdn.microsoft.com/en-us/library/bb934049.aspx
- BitLocker and Encrypting File System (EFS) for full logical volume encryption
  - https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

Encryption in transit

- IPsec secures the insurance provider's network communications by encrypting data transmitted over the network
  - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc740240(v=ws.10)
- TLS/SSL offer privacy and data integrity in transmission between servers & browsers
  - https://msdn.microsoft.com/en-us/library/windows/desktop/aa380516(v=vs.85).aspx

Duck Creek Technologies paves a genuine path to the future for P&C insurance companies. Decades of insurance experience underpin advanced technologies specifically designed to accommodate change - allowing carriers to navigate uncertainty and capture market opportunities faster than their competitors. Duck Creek solutions are available standalone or as a full suite. All are cloud-ready.

35 Great St Helen's
London
EC3A 6AP
United Kingdom

+44 (0)2078 989563

www.duckcreek.com