DATA PRIVACY AND SECURITY POLICY

Capital terms used in this Data Security Policy not defined in this document have the meaning assigned to those terms in the Draftomat Terms & Conditions.

Connection to Draftomat (including API access) is secure and encrypted using HTTPS with minimum TLS version 1.2. Templates, Best Practice Content and Documents are stored and encrypted at rest using AES - 256-bit encryption. Draftomat stores file data at Azure Blob Storages. Azure Storage is geo-redundant storage with primary data centers in the West Europe region and secondary data centers in North Europe region for fallback purposes. Storage is not publicly accessible. It is only accessible from the same Virtual Network where API App Service is running by using the secure key access stored in Azure Key Vault.

Non-authentication data is managed and stored in Draftomat Databases. Draftomat Database data is also encrypted at rest by Azure Managed certificate (AES 256). Draftomat Database server is only accessible through private DNS zone and Virtual Machine residing in the same Virtual Network for database deployment purposes only. Draftomat developers have access to Virtual Machines through a private VPN network (from certain IP addresses only) on an as-needed basis only. Database access is secured with strong passwords and keys residing in Azure Key Vault. To keep passwords and keys secure, Draftomat uses Azure Key Vault.

User-authentication-related data (username, password, multi-factor authentication information) is completely handled by Azure Active Directory services and they are not stored in the Draftomat Database and Draftomat staff cannot view user's password. If a user forgets their password, they must go through the reset procedure to be able to access their account again. Passwords that are used for sharing functionalities are hashed with HMAC algorithm (RFC 2104) using the SHA-256 hash function (FIPS 180-4) and salted with 128bit salts.

Draftomat production environment is completely isolated from other environments — including development and testing.

When working on a support issue Draftomat team does its best to respect users' privacy as much as possible and only accesses minimum data needed to resolve the issue.

Privacy of Customer's and Suborganization's data is ensured. Templates, Best Practice Content and Documents stored in the Draftomat Galaxy portal are not accessible to Draftomat staff through Draftomat Galaxy portal. Equally, Documents created by Suborganization are not accessible through Draftomat portal to the Customer who uses Draftomat to sell a service to the Suborganization. Customer decides what other information (User and groups details, Customer details, Licenses duration, License type and License allocation to suborganization) it wants to share with Legaltech through Sensitive data settings.