templafy

Templafy Sub-processors

September 2025

Table of Contents

1. Introduction

> Templafy takes great responsibility for safeguarding the right to privacy by embedding trust and transparency at the core of our culture. We employ state of-the-art measures to protect the personal information entrusted to us.
>
> ***Margrét Due***
> *Head of Privacy*

Templafy is committed to grant optimal protection to customer data, and that this protection travels with the data wherever it goes. We partner only with trusted providers for the purpose of delivering a best-in-class content enablement platform.

The sub-processors in use for our service are subject to due diligence on the information security practices and data protection compliance. Each sub-processor is required to commit to written obligations regarding their security controls and applicable regulations for the protection of personal data. We have thoroughly vetted their data protection and security measures to ensure that they meet the same high standards that we hold ourselves to.

This whitepaper provides information about the sub-processors in use for the Templafy services. Due to our uniform offering across the customer base, the sub-processors apply to all Templafy customers, unless where otherwise specifically mentioned. You will find information about the security measures that are implemented to ensure there is no compromise in the protection of your data, as well as the scope of processing activities assigned to each sub-processor for the purpose of delivering high-quality customer centric services to you.

2. List of sub-processors

Made available and updated on our website

Type	Entity	Sub-processing purpose	Country
Infrastructure Sub-Processors	Microsoft Irleand Operations Ltd.	Cloud service provider	One: Ireland and the Netherlands; Hive: Ireland, the Netherlands and as selected by customer: Sweden, United States, Canada or Australia
	Twilio, Inc.	SendGrid services for email notifications	United States
Service Sub-processors	Omnidocs A/S	Template creation services (only per Customer request)	Denmark
	Zendesk, Inc.	Customer support platform	Ireland
	Amplitude, Inc.	Analytics on product use	Germany
	Salesforce, Inc.	Customer success platform (CSP)	Sweden
	Keepit A/S	Backup service for CSP	Germany
	Skilljar, Inc.	Customer training platform	United States
AI/LLM Sub-processors	Microsoft Irleand Operations Ltd.	Enabling AI-based functionalities powered by Azure AI Vision and Azure OpenAI, involving prompt processing and generation of model outputs	Available in EU, United States, Canada, Australia: • AI Assistant • Data Transformation • Search Available in EU, United States: • Document Agents
Templafy affiliates	Templafy Inc.	Service provisioning	United States
	Templafy ApS	Service development, maintenance and provisioning	Denmark
	Templafy Deutschland	Service development, maintenance and provisioning	Germany
	Master IT Solutions B.V. (Templafy Eindhoven)	Service development, maintenance and provisioning	The Netherlands
	Templafy Limited	Service provisioning	United Kingdom
	Templafy LLC	Service provisioning for customers contracting directly with this entity	United States
	Templafy Australia Pty Limited	Service provisioning for customers contracting directly with this entity	Australia

3. International Data Transfers

Adequacy decision and standard contractual clauses

GDPR perspective

The European Commission adequacy decision based on the EU-U.S. Data Privacy Framework (DPF) has determined that U.S. laws now offer sufficient protections in terms of transparency, necessity and proportionality to mitigate the impact of U.S. signals intelligence activities. This framework creates greater legal certainty about U.S. data transfers and make our transfer impact assessments (TIAs), and in turn TIAs of our customers, more robust and seamless. Following the latest guidelines on adequate data protection, Templafy has certified its U.S. entity under the DPF program, and holds its critical sub-processors to the same standard. Section 4 lists the legal method for transfers to third countries and international organizations, for each sub-processor.

In addition to the EU GDPR Article 45 adequacy decision as a legal method for transferring data outside the European Union, Templafy ensures that the standard contractual clauses (SCCs) dated 4 June 2021 (or as otherwise updated or amended) are incorporated into each sub-data processing agreement (DPAs). TIAs are performed to evaluate the level of data protection in the third country destination of the data, as well as the need to implement additional safeguards.

Templafy has implemented numerous organizational, technical and contractual measures to ensure secure data handling is of utmost priority, including multiple measures in the product and in the company at large with our ISO27001, ISO27017 and SOC II achievements. Please visit our security and privacy trust center to review our latest compliance documentation attested to by third-party auditors. All Templafy customers have the right to stop transfers if they believe our response is not sufficient. This may mean some functional or support services becomes unavailable.

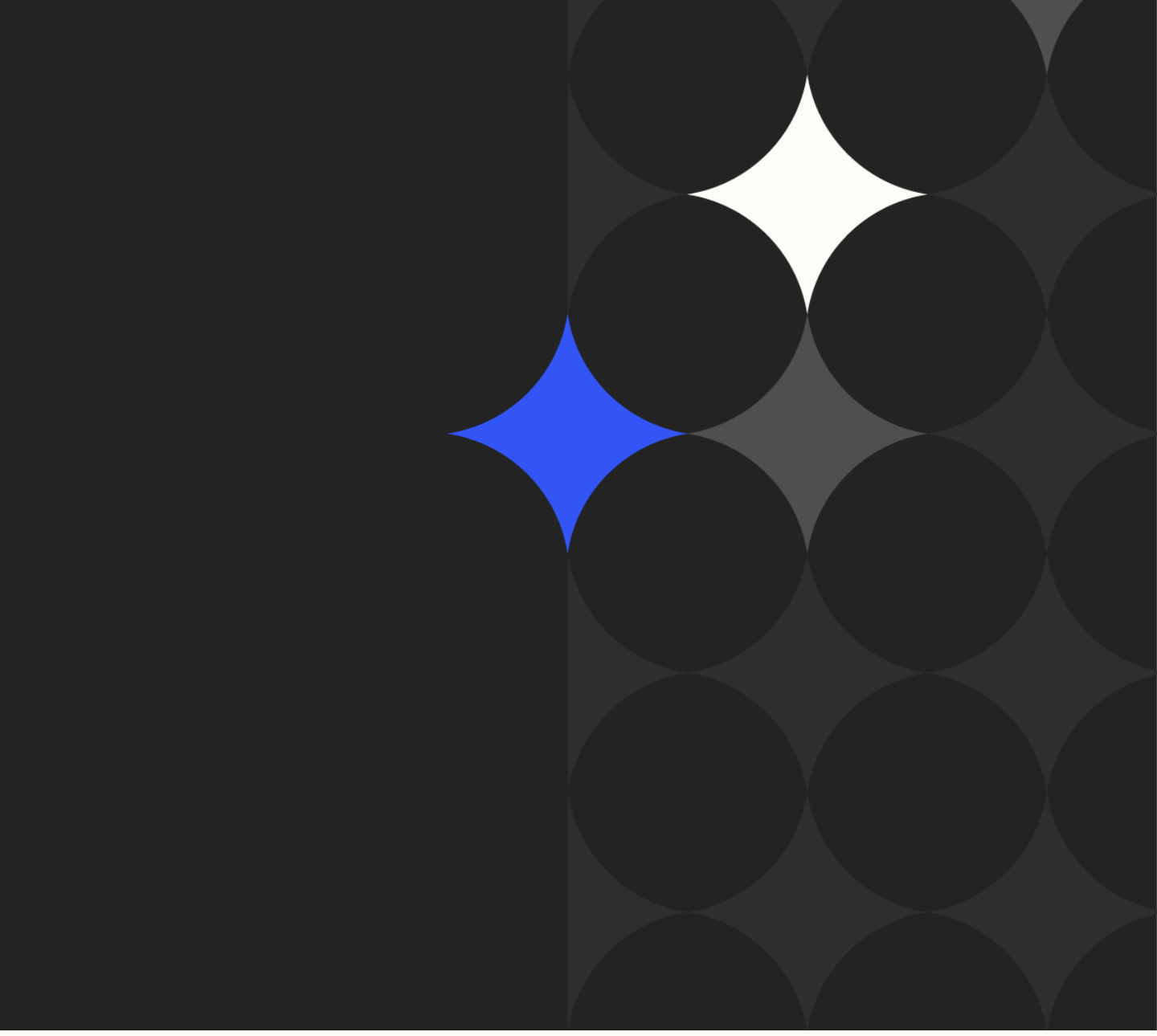
3. International Data Transfers

Transfer impact assessment

GDPR perspective

The SCC and TIA legal framework for data transfers outside the European Union emphasizes the importance to consider not only the legal framework of the jurisdiction of the data importer, but also practical experience with relevant prior instances of requests for access received from public authorities outside the EEA. Templafy does not provide assistance to U.S. authorities conducting surveillance activities. We are constantly looking for proportionality between identified risks, appropriate and supplementary measures, circumstances of the processing and acceptable residual risks, as well as proportionality between personal data processed and the purpose of such processing. Thus, the objective of performing a risk assessment of any type of data collection, storage and processing is not to eliminate risk, rather to assess, minimize and manage the risks on an ongoing basis. Templafy reviews and where necessary adapts supplementary measures it has implemented at least once per year to address data protection regulatory developments and risk environments. High-level list of these measures are listed for each sub-processor in section 4.

Templafy has no reason to believe that it will be subject to upstream surveillance orders by U.S. authorities. Templafy does not provide internet backbone services, but, instead only carries traffic involving its own customers. As of September 2024, Templafy has received zero requests for customer information from law enforcements, and we make our up-to-date transparency report available here. In terms of Templafy sub-processors, Templafy is of the opinion that the U.S. authorities would not request data directly from Templafy's sub-processors, because our sub-processors have limited or no ability to associate data with a specific customer or user. Accordingly, Templafy expects that U.S. authorities would request information directly from Templafy, not from our U.S. sub-processors.



4. Sub-processor details

This section provides information about each third-party sub-processor in use for the services, their assigned processing activities and the safeguards implemented for personal data protection.

Microsoft (Infrastructure)

Entity legal name	Microsoft Ireland Operations, Ltd.
Entity registered address	• Microsoft Ireland Operations, Ltd. South County Business Park, One Microsoft Place, Carmanhall And Leopardstown, Dublin, D18 P521, Ireland • Microsoft Corporation (HQ), One Microsoft Way, Redmond, WA 98052, United States
Business registration number	DUNS number: 08-146-6849, Chamber of commerce number: E256796
Sub-processing purpose	Cloud service provider
Data processing description	Microsoft Azure Platform-as-a-Service hosts the Templafy Software-as-a-Service. Personal data in the customer's user profiles, digital assets on their Templafy tenant, and usage data is processed continuously as Templafy delivers the SaaS to the customer.
Data types	Name, business email address, business phone number, job title, office location and other similar contact information as determined by customers; documents, images and other content or data in electronic form stored or transmitted by users via the services; product usage information; roles and other authentication and security credential information
User scope	All customer's assigned users
Data hosting country	The Netherlands and Ireland and (as selected by customer) Sweden, United States, Canada or Australia.
Third country transfer governance	Adequacy decision under DPF participation and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Microsoft
Privacy contact information	• Address: Microsoft Ireland Operations, Ltd., Attn: EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopards town, Dublin 18, D18 P521, Ireland • Email: DPOffice@Microsoft.com • Telephone: +353 1 7063117 Inquiries can be submitted here
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Microsoft's DPA includes clauses for governing data requests from authorities, sub-processor restriction and onward control using SCC to their sub-processors • Microsoft will not move or replicate content outside of the applicable region without prior agreement, except in each case as necessary to comply with the law or a binding order of a governmental body • Azure implements strong encryption for data both in transit (TLS 1.2+) and at rest (AES 256), comprehensive compliance with global privacy laws, and user control over data location and access • Cryptography keys are reliably managed as defined by the GDPR and Schrems II recommendation 1/2020 point 84 • Microsoft adheres to the main privacy standards, laws and regulations including: GDPR, ISO/IEC 27701, ISO/IEC 27018, HIPAA, HITRUST, FERPA. • For transparency on how Microsoft handles customer data, ensuring that privacy is integrated into its cloud services from the ground up, please visit the Microsoft Azure privacy page and the relevant security collateral can be found here.

Microsoft (AI/LLM)

Entity legal name	Microsoft Ireland Operations, Ltd.
Entity registered address	• Microsoft Ireland Operations, Ltd. South County Business Park, One Microsoft Place, Carmanhall And Leopardstown, Dublin, D18 P521, Ireland • Microsoft Corporation (HQ), One Microsoft Way, Redmond, WA 98052, United States
Business registration number	DUNS number: 08-146-6849, Chamber of commerce number: E256796
Sub-processing purpose	Enabling AI-based functionalities that enhance content management and document automation, such as tagging, data transformation, writing assistance, and dynamic field generation. These features require processing of user-provided inputs to deliver their functionality and may include tokenization and temporary model inference.
Data processing description	User-provided data is temporarily processed in the selected region to generate AI-driven outputs, such as tags, rewritten content, suggested text, or dynamic field values. Data is sent for real-time inference only, without storage or used for model training. Features are optional, triggered by users, and managed by administrators.
Data types	User-provided text, document content, metadata, and file elements (e.g. images or field values) that may include personal data depending on customer input and configuration. More details on each AI feature can be found here.
User scope	All customer's assigned users
Data hosting country	Available in EU, United States, Canada, Australia: • AI Assistant • Data Transformation • Search Available in EU, United States: • Document Agents. More details on each AI feature can be found here.
Third country transfer governance	Adequacy decision under DPF participation and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Microsoft
Privacy contact information	• Address: Microsoft Ireland Operations, Ltd., Attn: EU Data Protection Officer, One Microsoft Place, South County Business Park, Leopards town, Dublin 18, D18 P521, Ireland • Email: DPOffice@Microsoft.com • Telephone: +353 1 7063117 Inquiries can be submitted here
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Microsoft's DPA includes clauses for governing data requests from authorities, sub-processor restriction and onward control using SCCs to their sub-processors • No personal data is used to train Microsoft or AI models. • Abuse monitoring is automated, with human review only triggered if content cannot be reviewed by automated systems • Azure implements strong encryption for data both in transit (TLS 1.2+) and at rest (AES 256), comprehensive compliance with global privacy laws, and user control over data location and access • Azure OpenAI is deployed within Microsoft's enterprise-grade compliance framework, including: GDPR, ISO/IEC 27701, ISO/IEC 27018, HIPAA, HITRUST, FERPA. • For details on Microsoft's reviewer safeguards, read more here. • For transparency on how Microsoft's data handling and built-in privacy read more here and here.

Twilio

Entity legal name	Twilo Inc.
Entity registered address	1801 California Street, Suite 500, Denver, CO 80202, United States
Business registration number	CAGE code: 7CDP5
Sub-processing purpose	SendGrid services for email notifications
Data processing description	Service email notifications sent through the services as customer users make use of functionality in their Templafy tenant, such as inviting users, assigning roles, resetting password.
Data types	Name, work email address, email system activity
User scope	All customer's assigned users
Data hosting country	United States
Third country transfer governance	Adequacy decision under DPF participation and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Twilio
Privacy contact information	• Address: Twilio Inc., Attn: Office of the Data Protection Officer, 101 Spear St, Ste 500, San Francisco, CA 94105, United States • Email: privacy@twilio.com • DPO/chief privacy responsible: Amy Holcroft, Chief Privacy Officer
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Data minimization is in place, the emails are not stored • Data is encrypted in transit with opportunistic TLS (minimum 1.2) • Security by design is implemented across the entire product lifecycle • Identity and access management controls are in place and MFA is implemented • Twilio will inform of data breaches without undue delay • Twilio has achieved security certifications and attestations such as: ISO/IEC 27001, 27017, 27018, SOC 2 Type II and PCI-DSS Level 4 • Learn about Twilio's security here

Zendesk

Entity legal name	Zendesk, Inc.
Entity registered address	989 Market St San Francisco, CA 94103, United States
Business registration number	CAGE code: 798G5
Sub-processing purpose	Customer support platform provider
Data processing description	Personal data in support tickets and related to support requestee upon customer use of Templafy support via support@templafy.com
Data types	Email, and any other information submitted within the ticket to support the customer service team
User scope	Users who submit support tickets, any users that may included in copy or free text of support tickets
Data hosting country	Ireland
Third country transfer governance	Adequacy decision under DPF participation and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Zendesk
Privacy contact information	• Address: Zendesk, Inc., Attn: Privacy Team and DPO. 989 Market Street, San Francisco, CA 94103, United States • Email: privacy@zendesk.com, euprivacy@zendesk.com • DPO/chief privacy responsible: Alex Wall, Director, Senior Privacy Counsel
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Data minimization is in place • Role-based access control is implemented • Data is encrypted in transit (TLS 1.2+) and at rest (AES 256) • Zendesk has 24/7 monitoring in place • Zendesk will inform of data breaches without undue delay • Zendesk adheres to the main security and privacy standards, laws and regulations including: SOC 2 Type II, ISO 27001, ISO 27018, ISO 27701, FedRAMP LI-SaaS, PCI-DSS, HIPAA, HDS • Learn about Zendesk security here

Amplitude

Entity legal name	Amplitude, Inc.
Entity registered address	201 3rd Street, Suite 200. San Francisco, CA 94103. United States
Business registration number	IKRS Employer Identification Number: 45-3937349
Sub-processing purpose	Analytics on product use and effectiveness of our services, to improve and add features to our service and improve the content and functionality of the services
Data processing description	Pseudonymized data about customer use of services provided as end-users navigate through the SaaS (usage analytics)
Data types	User ID (pseudonymized), product usage information
User scope	All customer's assigned users
Data hosting country	Germany
Third country transfer governance	Adequacy decision under DPF participation and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Amplitude
Privacy contact information	• Address: Amplitude, Inc., Attn: Privacy, 201 Third Street, Suite 200, San Francisco, CA 94103, United States • Email: privacy@amplitude.com • DPO/chief privacy responsible: Heather Dunn Navarro, VP, Deputy General Counsel, Product & Privacy
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Personal data in the application is pseudonymized • Role-based access control is implemented and data minimization is in place • Amplitude will inform of data breaches without undue delay • Amplitude adheres to the main security and privacy standards, laws and regulations including: GDPR, CCPA, HIPAA, ISO 27001, ISO 27018 and SOC 2 Type II • Learn about Amplitude security here

Salesforce

Entity legal name	Salesforce, Inc.
Entity registered address	Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States
Business registration number	Legal Entity Identifier (LEI):RCGZFPDMRW58VJ54VR07, Registration authority entity ID: 2991326
Sub-processing purpose	Customer success and product engagement tool
Data processing description	Contact information and information about product use processed to provide tailored service and support to customers
Data types	Name, email address, phone number, job title, work address and as otherwise determined by customer admins and users, as well as usage data related to the services provided to customers.
User scope	All customer's assigned users
Data hosting country	Sweden
Third country transfer governance	Adequacy decision under DPF participation, Salesforce processor binding corporate rules and the standard contractual clauses
Sub-DPA	Standard data processing agreement - Salesforce
Privacy contact information	• Address: Salesforce Inc. Attn: Salesforce Data Protection Officer (Salesforce Privacy Team) (and in India, a Grievance Officer), 415 Mission St., 3rd Floor, San Francisco, CA 94105, United States • Email: privacy@salesforce.com • DPO/chief privacy responsible: Lindsey Finch, Exeecutive Vice President, Global Privacy & Product Legal
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Role-based access control is in place. Access happens through SSO and MFA is supported • Data minimization and purpose specification is in place • Salesforce ensures data security through TLS 1.2+, unique identifiers for user sessions, and secure server environments with firewalls. It mandates AES128 or AES256 encryption for outbound calls to maintain high security standards • Data backup and recovery • Salesforce will inform of data breaches without undue delay • Salesforce adheres to the main security and privacy standards, laws and regulations including: SOC 2 Type II, ISO 27001, ISO 27018, ISO 27701, FedRAMP High, PCI-DSS, HIPAA, HITRUST, HDS, TISAX • Learn about Salesforce security here

Keepit

Entity legal name	Keepit A/S
Entity registered address	Per Henrik Lings Allé 4, 7th, 2100 Copenhagen, Denmark
Business registration number	CVR: 30806883
Sub-processing purpose	Backup services for the cloud success platform (CSP)
Data processing description	Backup provider for Salesforce
Data types	Name, work email address, work phone number, job title, office location, and as otherwise determined by customers in configuration and use of the services. Same scope as Salesforce.
User scope	All customer's assigned users
Data hosting country	Germany
Third country transfer governance	Standard contractual clauses
Sub-DPA	Standard data processing agreement - Keepit
Privacy contact information	• Address: Keepit A/S, Per Henrik Lings Allé 4, 7th, 2100 Copenhagen, Denmark • DPO: Ariana Lepia • Email address: dpo@keepit.com
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • Keepit does not share infrastructure with any public cloud • Data is encrypted in transit (TLS 1.2+) and at rest (AES 256) • The application does not expose any APIs or other means that allow data overwrites. The application uses a blockchain algorithm which makes any low-level tampering impossible and easily evident • Keepit may not transfer data outside the EU without Templafy's explicit consent • Keepit will inform of data breaches without undue delay • Keepit is ISO/IEC 27001 certified • Learn about Keepit security here

Skilljar

Entity legal name	Skilljar, Inc.
Entity registered address	720 Olive Way Ste 700, Seattle, Washington, 98101, United States
Business registration number	DUNS: 079423702
Sub-processing purpose	Customer training platform
Data processing description	Personal data collected to provide customer training
Data types	Email, name, job title, training analytics (course progress)
User scope	Customer admins upon registration, as well as any end-users assigned by customer admins
Data hosting country	United States
Third country transfer governance	Standard contractual clauses
Sub-DPA	Standard data processing agreement - Skilljar
Privacy contact information	• Address: Skilljar Inc., 113 Cherry Street, Suite #29434, Seattle, WA 98104, United States • Email: legal@skilljar.com • DPO/chief privacy repsonsible: Jason Stewart, security@skilljar.com
Additional suitable guarantees	• Templafy carries out periodic reviews of supplier security measures • This sub-processor is only applicable upon customer admin, super-admin or owner opt-in • Data minimization is in place • Role-based access control is implemented • Data is encrypted in transit (TLS 1.2+) and at rest (AES 256) • Skilljar will inform of data breaches without undue delay • Skilljar adheres to the main security and privacy standards, laws and regulations including: GDPR and SOC 2 Type II • Learn about Skilljar security here

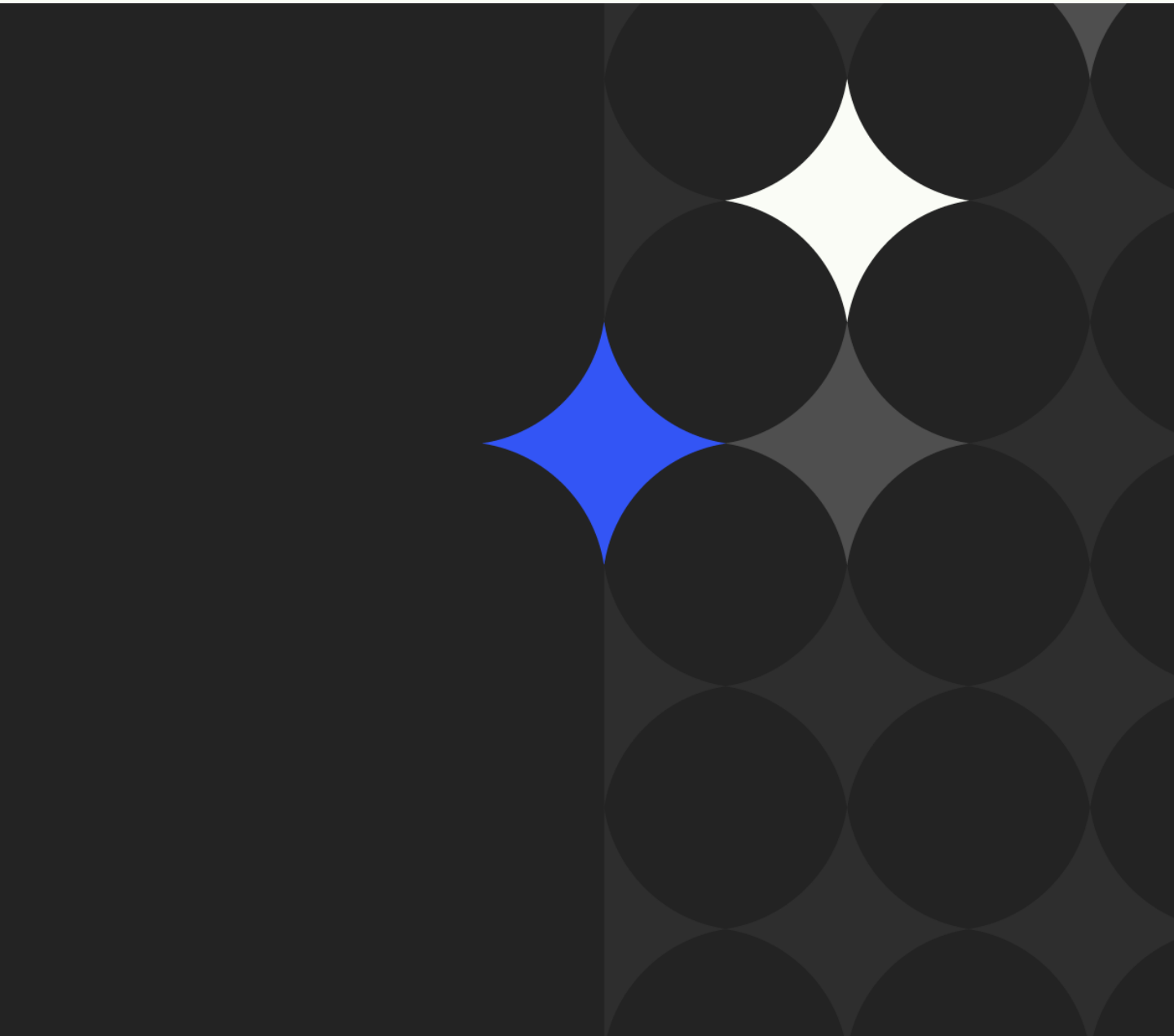
8. Conclusion

Templafy carefully selects sub-processors with the objective of maximizing customer satisfaction with our software-as-a-service, while preserving the protection of data entrusted to us. Templafy's information security and privacy team is dedicated to ensure only trustworthy sub-processors are onboarded; that we're on top of the dynamic landscape of regulations and requirements; and that we are security and privacy first in everything we do. If you have any questions, don't hesitate to reach out to us.

Sincerely,

Templafy Privacy

privacy@templafy.com



www.templafy.com