Notified Global Privacy Compliance Guide

Effective November 2021

This document outlines some of Notified's core compliance processes with the Global Data Protection and Privacy Regulations.

Introduction

Notified has a comprehensive Privacy and Data Protection compliance program that, among other things, outlines Notified's processes in relation to demonstrating compliance (privacy by design, privacy impact assessments on our services, data mapping, privacy audits, updating our customer contracts and training videos), retention policies (data minimization, data accuracy, record keeping, and access rights), security (ensuring accuracy and meeting ISO27002 standards), notification policies (breach notification procedures) and subcontracting (ensuring our subcontractors meet our privacy and security minimum standards).

Notified acts as a "data processor" in relation to the personal data from customers or on behalf of customers, and each customer remains the "data controller" with respect to such personal data. There are a number of obligations on data processors under privacy law. Notified and its affiliate companies that process personal data of individuals ("Notified" or "we") have implemented the measures outlined in this document.

GDPR & CCPA

The GDPR applies to any business that acts as data controller or data processor and offers goods or services to individuals in the European Union ("EU"), regardless of whether it is physically located in the EU.

The CCPA applies to any business inside or outside of California who collects consumer personal data of California State residents.

Processing Personal Data

Notified conducts privacy impact assessments on its services, systems, platforms, databases, processes, and vendors. We keep records of data processing activities and a personal data inventory. We also incorporate policies such as data minimization, privacy by design and pseudonymization into our privacy processes.

Notified integrates data privacy into its information security policy by including storage and limitation, encryption, integrity and confidentiality, breach notifications and transparency. Notified implements regular security risk assessments, data quality procedures, tools for data de-identification and an encryption policy. We have policies and procedures to ensure personal data is accurate and up to date. For inaccurate data, the data is erased, updated or otherwise rectified.

Notified obtains valid grounds for processing personal data from customers via customer contracts, order forms and/or website terms and conditions. We keep an internal database of executed contracts and order forms. We also maintain a data inventory that sets out on what ground we rely on when processing personal data.

Data Breach Notification Procedures

Notified has data breach notification procedures to ensure it notifies customers where required and in accordance with applicable law and customer contract obligations. Notified has a breach response plan to ensure compliance with

applicable law with respect to timing requirements for notification and the content of a notification letter. The breach response plan requires maintenance of a log to track data breaches. Notified conducts data breach response testing and we maintain data breach metrics. Documentation outlining Notified's data breach notification procedures and incident response plan is available upon request and will be disclosed under contracted confidentiality obligations.

Privacy Statement

Notified has a privacy statement that details our personal data handling processes. The privacy statement is an external-facing notice of Notified's processing activities. It further ensures the required information is provided to data subjects when their information is collected such as secondary uses of personal data.

The privacy statement addresses the following:

- How Notified can respond to access requests in a timely and appropriate manner;
- Purpose of processing personal data;
- Categories of personal data;
- Recipients of personal data;
- Data storage periods;
- Rights to rectification and complaint;
- Sources of data; and
- Safeguards for transfer to third countries.

The Privacy statement is available online: www.notified.com

Right to be Forgotten, Corrections, Transparency and Portability

Notified has procedures to respond to requests to be forgotten or for erasure of data. Notified ensures to delete personal data when data is no longer necessary for processing unless we are required to retain the data for a longer period of time as required by applicable law. We have processes in place to ensure records of personal data are used in line with any restrictions, and respond to requests to opt-out, restrict or object to processing. Notified has a data retention policy available upon request and will be disclosed under contracted confidentiality provisions. It outlines time frames for the erasure or pseudonymization of customer personal data.

Customers' personal data is not kept for longer than is necessary to accomplish the purpose for which it was collected. Notified undertakes to do the following:

- Review the length of time it retains personal data;
- Securely delete personal data no longer needed for a specific purpose; and
- Update, archive or securely delete personal data if it becomes out of date.

Notified maintains procedures to respond to requests to update or correct customer personal data, and has technical solutions in place for processing data portability requests.

Audits and Privacy Impact Assessments

Notified has implemented appropriate technical and organizational measures to ensure and be able to demonstrate compliance with applicable laws such as GDPR and CCPA. These measures include, but are not limited to, privacy

impact assessments and data mapping of products, solutions, databases and projects ("PIAs"), annual internal privacy audits, data inventory lists, data breach assessments and information security testing (together, "Audit Measures").

Notified takes Audit Measures on certain new programs, products, systems, databases and processes. Notified engages internal stakeholders from relevant departments when conducting Audit Measures, which take into account the following:

- A description of the processing activities being assessed;
- An assessment of the risks to data subjects; and
- A description of the measures Notified takes to address risks, including safeguards, security measures and mechanisms Notified will implement to ensure global privacy and data protection compliance. We then track and address data protection issues or risks.

The objective of a PIA is to assess Notified's privacy protection position against any legislative, contractual requirements and international best practices and to review compliance with Notified's own privacy policies. The scope of a PIA involves evaluating procedures undertaken by Notified throughout the typical information life-cycle phases: how data is created or received, distributed, used, maintained and disposed of or deleted.

Audit Measures guarantee data protection risks are measured, analyzed and mitigated and they enable Notified to identify issues and risks and determine, based on the likelihood and impact, where to prioritize resources to mitigate risk. Audit Measures also ensure the ability for Notified to demonstrate appropriate technical and organizational measures have been put in place for compliance with GDPR.

Privacy by Design

Notified integrates privacy by design into our systems and product development. Examples of privacy by design include application development protocols, security risk assessments, software for aggregation, data masking and pseudonymization, encryption and anonymization. Notified implements data protection by default into our security, product and operational processes.

Notified anonymizes personal data in which direct and indirect personal identifiers are removed and technical safeguards are implemented such that the personal data can never be re-identified so there is zero re-identification risk.

In some cases, Notified pseudonymizes or encrypts processing of personal data in such a way the data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to technical and organizational measures to ensure the personal data is not attributed to an identified or identifiable natural person.

Sub-Contracting and Third Party Vendors

Notified only appoints sub-contractors who have sufficient guarantees to implement appropriate measures to guarantee compliance with applicable law and with a contract that governs the relationship. We provide information security and privacy screening questions for potential sub-contractors and other processors, as well as maintaining lists of sub-contractors that process our personal data, which are available to customers, employees and supervisory authorities upon request.
Notified appoints sub-contractors under a binding written agreement, which requires sub-contractors only act on Notified's instructions and ensure the security of Notified's personal data it processes. At a minimum, Notified's binding written agreement stipulates sub-contractors must:

- Only act on Notified's documented instructions;

- Impose confidentiality obligations on all personnel who process the relevant data;
- Ensure the security of the personal data it processes;
- Not send personal data to third party suppliers or impose the same data protection obligations on its third party suppliers without our approval; and
- Implement measures to assist Notified in complying with the rights of data subjects.

Notified conducts regular due diligence, audits and assessments on its sub-contractors to ensure compliance with applicable law and general data protection and security obligations. Notified requires its sub-contractors to keep personal data they process confidential.

SECURITY

Notified implements physical, administrative and technical security measures. If Notified learns of a security breach involving personal data, when required by law or contract, we notify the affected customer so appropriate protective steps can be taken. Notified is not responsible for unauthorized access to such personal data by hackers or others that obtain access through illegal measures, in the absence of negligence on the part of Notified. Notified's information security policy incorporates the ISO 27002 information security framework.
The following security measures are implemented by Notified:

- technical security measures such as intrusion detection, firewalls, encryption and monitoring;
- on-going tests and reviews of security measures;
- redundancy and back-up facilities;
- processes to restore availability of and access to personal data in the event of an incident;
- password parameters, data centre security measures, identity access management and restrictions on accessing personal data;
- audits and tests on information on Notified's internal security processes and Notified's sub-contractors information security processes;
- information security incident/breach response plan; and
- data logging to track all data privacy incidents and breaches.

Notified has a dedicated information security team that assists the business globally.

DATA PROTECTION OFFICERS AND REGISTRATION WITH A SUPERVISORY AUTHORITY

Notified has a designated data protection officer ("DPO") in order to comply with Article 37 of GDPR. Additionally, Notified has a dedicated privacy and data protection team of legal professionals ("Privacy Office") who is responsible for Notified's compliance with applicable data privacy legislation and contractual obligations. The Privacy Office may be contacted via email at privacy@notified.com.

For the purposes of GDPR compliance, Notified's lead supervisory authority in the EU is in Sweden.

CROSS BORDER DATA TRANSFERS

Notified, it affiliates and sub-contractors may process customer personal data in the United States, the United Kingdom, the European Union, Canada, India, Philippines and the rest of the world and may be transferred outside the country in which a customer provided such personal information.

Notified's PIAs, TIAs and data mapping maintain logs and records of the personal data transfers. The basis for such transfers includes but are not limited to:

- services reservation, set up and delivery, pre and post-call services;
- support, maintenance and resolution of customer queries;
- account set-up and account management;
- invoicing and collections purposes;
- records and internal administration;
- business reporting and statistical analysis;
- complying with legal obligations of the data exporter and/or the data importer; and
- cooperating with respect to actual or prospective legal proceedings, inquiries and investigations of governmental, judicial or regulatory authorities.

Notified and its affiliates also use EU standard contractual clauses as a valid data transfer mechanism.

Global Privacy Training

Notified provides its employees with mandatory privacy compliance and security training and awareness. Such training and awareness outline the processes and procedures for protecting and managing data, information, and information systems under GDPR, CCPA and all other applicable privacy and data protection laws. Attendance and comprehension are tracked.

Conclusion

Notified proactively monitors future developments in EU and global privacy laws, including best practices. Notified may at any time update or modify its privacy and data security processes. The information contained herein has been prepared for general information purposes only to permit you to learn more about Notified's privacy and data protection processes. The information presented is not legal advice, is not to be acted on as such, may not be current and is subject to change without notice.

Need More Information?

The Privacy Office may be contacted via email at privacy@notified.com.