General Data Protection Regulation (GDPR) Compliance Information

Introduction

Internap Corporation ("INAP"), together with its domestic and foreign subsidiaries (collectively, "INAP"), provides high-performance data center services including colocation, managed hosting, cloud, and network services across a global network of data centers and POP locations. INAP customers may use INAP services to store, transmit, encrypt, decrypt, modify, process and otherwise manipulate or transmit data. In most cases, INAP does not directly control how its services and infrastructure are utilized and what information is stored on or transmitted through such infrastructure.

Certain of this data may constitute protected "personal data" as that term is defined in the E.U. General Data Protection Regulation ("GDPR"). In addition, certain of the INAP services may constitute "processing" as that term is defined in GDPR. As such, GDPR may apply to INAP in certain circumstances, depending on the services provided and data stored.

The following disclosures concerning INAP's compliance with GDPR are presented for informational and compliance purposes only. Nothing in these disclosures constitutes a representation that any particular data or service is governed or subject to GDPR, nor do these disclosures represent or constitute any contract or undertaking with any customer or prospective customer.

Effective Date of GDPR

GDPR is set to take effect on May 25, 2018. On and after that date, INAP will comply with GDPR to the extent applicable.

INAP's Status Under GDPR

Under GDPR, INAP may be designated as (i) a "controller" subject to GDPR with respect to certain data sets; (ii) a "processor" subject to GDPR with respect to certain data sets; or (iii) not subject to GDPR for certain data sets.

Processor

If GDPR applies, in most cases, INAP will be a "processor." This means that INAP will store or perform some other set of operations on a data set that contains "personal data" for a customer, at the customer's written direction.

Example: INAP provides managed services hosting to Customer A, a retailer based in France. This customer stores shoppers' names, birthdates, email addresses and credit card information and many of these shoppers are EU citizens. Customer A is a "controller" of the shopper data. In connection with the managed services hosting, INAP has logical access to the shopper data, and therefore, INAP is a "processor" of the shopper data. INAP processes data for Customer A pursuant to a processor agreement.

Controller

INAP also collects and stores contract information, payment information, employee records, and other information for the purposes of conducting business, marketing, employment, and more. In these cases, INAP is a controller of data.

Example: INAP enters into a contractual agreement with Customer B concerning the use of colocation space. Customer B is based in the E.U. INAP receives personal information regarding employees of Customer B during negotiations, including the employees' work email addresses. INAP is a "controller" of this data.

GDPR Does Not Apply

For other relationships, GDPR will not apply, either because the data does not constitute protected data, or because the customer is not subject to GDPR.

Example: A US-based customer purchases managed hosting services for marketing data concerning US citizens. GDPR does not apply.

Example: An EU-based customer purchases colocation services from INAP. INAP does not have logical access to any customer data. INAP does not have a login, passwords, or any other data, and cannot access the server. INAP provides only physical security of the actual machine storing the data. INAP is not a data processor because INAP does not perform any operation on the customer's data. It is not necessary to execute a processor agreement with INAP under GDPR.

Example: An EU-based customer purchases network services from INAP. INAP does not have logical access to any customer data in connection with network services. It is not necessary to execute a processor agreement with INAP under GDPR, because INAP is acting as a "mere conduit" of the data and is not considered a processor of the data (See GDPR Article 2[4]).

INAP Responsibilities

Security: INAP implements standard up-to-date security measures to secure the environment and connections through which INAP provides its services. INAP can deliver additional and/or alternative measures upon customer's request.

Disclosure: INAP will not disclose any information to any third party unless authorized by law, or authorized by either the data subject, controller, or processor as the case may be.

INAP Compliance As Processor

If INAP is a "processor" under GDPR for a particular data set, INAP will enter into a processor agreement or data processor addendum. This agreement is required by GDPR and governs the terms of INAP's processing of the protected data at issue.

INAP Compliance As Controller

If INAP is a "controller" under GDPR, INAP will comply with applicable GDPR obligations. These include, but are not limited to the following:

INAP will lawfully process data.

INAP will enter into processing agreements with any third-party processors prior to sending personal data to such processors.

INAP will maintain all required records and provide required modalities for the exercise of rights of the data subject.

INAP will retain data only as long as necessary for the purpose for which it was obtained.

INAP will provide required notices.

INAP will adopt all required policies and procedures and train employees who handle personal data governed by GDPR.

INAP will implement privacy by design and privacy by default with regard to personal data governed by GDPR.

INAP will provide all required notifications in the event of a data breach.

GDPR Compliance

To ensure GDPR Compliance, INAP undertakes the following:

INAP enters into data processing agreements with its customers if GDPR applies to the processing of their data.

INAP enters into sub-processing agreements with its providers if necessary.

INAP maintains all documentation required by GDPR and provides all required notices.

INAP maintains up-to-date security measures, performs regulator audits, and will implement additional security at the customer's request and pursuant to the terms of applicable agreements.

In areas applicable to GDPR, INAP offers its customers assistance in relation to security, data subject rights, data breaches, data protection impact assessment, prior consultation, and other elements of GDPR.

For any further questions regarding this notification or INAP's compliance with GDPR more generally, please contact us at: GDPR@inap.com. Please be advised that INAP cannot respond to any questions regarding your status as a controller or processor.

Data Subject Notifications

As set forth above, in certain instances INAP will act as a controller under GDPR. Article 13 and 14 of GDPR require INAP to provide certain information to data subjects when collecting their personal data directly from them or from third parties (such as an employer).

This summary is for informational purposes only, and is qualified in its entirety by applicable privacy policies and terms of use provided elsewhere on this website and by INAP affiliates. In the event of conflict, the terms of the applicable privacy policy or terms of use shall govern.

Identity of the Controller

INAP and/or any of its domestic and foreign subsidiaries will constitute the controller for GDPR purposes in the event that the data in question is personal data under GDPR and is collected by INAP. If you have any questions or concerns regarding collection of your personal data, please contact GDPR@inap.com.

Purposes of Processing of Data

INAP may utilize personal data in a number of ways in order to meet obligations under various agreements, to pursue legitimate interests such as facilitating services pursuant to contractual agreements with entities, including providing services such as colocation, managed hosting, cloud, and network services. The legal basis for this processing generally will be that it is necessary for the legitimate interests outlined above, but other bases may include compliance with legal obligations or consent.

Recipients of Data

The recipients of personal data will depend in large part on the services being provided that require the processing of personal data. In many cases, the only recipients of such data will be employees of INAP who have committed themselves to confidentiality. In other cases, INAP may transmit such data to processors or other controllers as necessary to meet INAP's obligations.

Transfer Outside of EU/EEA

INAP may transfer personal data outside of the European Union or European Economic Area. When INAP does this, appropriate safeguards will be in place, such as Privacy Shield accreditation or the insertion of approved model clauses. INAP will only transfer personal data to foreign controllers and processors who meet these standards.

Duration of Storage

INAP will only store your data as long as required by the basis for processing. For example, INAP will only store personal data that is being processed pursuant to INAP's legitimate interest so long as such interest is present. If INAP is processing personal data based on consent, that consent may be withdrawn by you at any time. Please contact GDPR@inap.com to withdraw such consent.

Your Rights as a Data Subject

INAP is committed to fulfilling its obligations concerning the exercise of your rights under GDPR. Please be advised that you have the following rights under GDPR (to the extent GDPR applies to your personal data):

The right to request access to, rectification or erasure (*i.e.*, the right to be forgotten) of personal data or restriction of processing or to object to processing;

The right to data portability;

The right to lodge a complaint with a supervisory authority; and

In certain circumstances, the right to know the source of the data and whether the source was public.

Should you have any questions regarding the exercise of these rights, please contact GDPR@inap.com. INAP may provide additional information in communications directly with data subjects as necessary.

Last Revised: April 2018