The General Data Protection Regulation (GDPR) is a new European Union regulation to bring added protection to the personal data of citizens. Harmonizing existing data protection laws, it will place new obligations on bodies or companies holding and processing data.

All organizations, whether private companies or government bodies, will be subject to the regulations, even if they are not established within the EU. Communications service providers and their networks handle large amounts of diverse data and face a variety of threats. They need to put in place robust solutions that will help them meet the new requirements and ensure they protect their customers.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>The General Data Protection Regulation</td>
<td>3</td>
</tr>
<tr>
<td>Rights and requirements</td>
<td>4</td>
</tr>
<tr>
<td>Data Controllers and Processors</td>
<td>5</td>
</tr>
<tr>
<td>What it all means for Communication Service Providers</td>
<td>5</td>
</tr>
<tr>
<td>CSPs are both controllers and processors</td>
<td>6</td>
</tr>
<tr>
<td>CSPs have extra responsibilities</td>
<td>6</td>
</tr>
<tr>
<td>Multiple attack vectors – insiders, endpoints and networks</td>
<td>7</td>
</tr>
<tr>
<td>Who is responsible for compliance?</td>
<td>8</td>
</tr>
<tr>
<td>Get ready for GDPR</td>
<td>8</td>
</tr>
<tr>
<td>Identify where personally identifiable information (PII) data resides</td>
<td>8</td>
</tr>
<tr>
<td>Implement controls to protect PII</td>
<td>8</td>
</tr>
<tr>
<td>Update incident response processes</td>
<td>9</td>
</tr>
<tr>
<td>Conduct periodic reviews</td>
<td>9</td>
</tr>
<tr>
<td>Implement Role-Based Access Control</td>
<td>9</td>
</tr>
<tr>
<td>Nokia NetGuard Security</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>10</td>
</tr>
</tbody>
</table>
Executive summary

Threats to the security of data are constantly evolving and multiplying. With individuals increasingly transferring, uploading and sharing data on line with a host of service providers, the risks can only increase.

Safeguarding personal data protects the right to privacy of individual citizens, as well as safeguarding assets such as back accounts, access to credit and other financial information and transactions.

Communications service providers (CSPs) are attractive targets for attackers seeking unlawful access to sensitive data. With large volumes of data stored, transmitted or accessed at many locations in complex heterogeneous networks, CSPs are particularly vulnerable to attack.

To update the security offered to citizens, the European Union (EU) is introducing the General Data Protection Regulation (GDPR), a replacement for the Data Protection Directive 95/46/EC. It is designed to harmonize data privacy laws across the EU, to protect and empower all EU citizens’ data privacy, as well as reshape and improve the way organizations approach data privacy.

For citizens, the GDPR specifies a number of protections, including the right to be forgotten. This prohibits organizations from holding any data without prior approvals and they must delete data if requested by users. Data subjects may also obtain and transfer personal data from one data controller to another, in a safe and secure fashion. The GDPR also requires data holders to obtain explicit opt-in consent from customers before using their personal data.

The GDPR is also comprehensive, applying to the processing of personal data of citizens and residents of the EU, even if the processor isn’t established in the EU. In effect, the GDPR applies to any company marketing goods or services to EU residents and citizens, as well as to official government bodies.

Stiff penalties apply to breaches of the regulations, with non-compliance resulting in penalties of up to 4 percent of worldwide turnover or €20 million.

The GDPR specifies what to do, but not how to do it and it is up to the organization to put in place robust systems and procedures to meet the various articles of the regulation. Nokia provides solutions that offer comprehensive data protection for networks, allowing CSPs to meet all the requirements of the GDPR.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation due to take effect in May 2018.

As such, it replaces the 1995 EU Data Protection Directive (Directive 95/46/EC) and the Data Protection Acts of EU member states. The GDPR stipulates that all companies must adhere to strict processes and procedures when collecting and storing the personal data of EU citizens.

The main goal of the regulation is to unify and harmonize the national data protection laws across the EU, to strengthen the obligations on those who process the personal data of EU individuals and enhance the rights of EU individuals to protect their privacy. The GDPR affects all organizations which process personal data, whether private companies or official bodies.
The GDPR applies to Personally Identifiable Information (PII), defined “as any information relating to an identified or identifiable natural person”, known as a data subject. (Article 4 (1)). The GDPR broadly applies the definition of PII to include the storage of EU personal data such as email, and the transmission, collection, recording, organization, retrieval, alignment, combination, restriction, erasure, destruction and/or use of personal data.

As an example, this applies to communications sent through email, mobile text, social network direct message and other similar media.

All companies within the EU are subject to this regulation, regardless of where the data is stored and processed. The jurisdiction of the GDPR also covers businesses outside the EU which offer goods and services to EU residents.

Article 3 of the GDPR states that it applies to the processing of personal data of citizens and residents of the EU, even if the processor isn’t established in the EU. In effect, this Article of the GDPR means that these Regulations apply to any company marketing goods or services to EU residents and citizens. These include:

- EU States: Government entities that handle the personal data of citizens and residents of the EU are as subject to GDPR rules as any company.
- EU Companies: EU companies, since they are both located within the EU and handle transactional and personal data of EU citizens and residents, are expected to comply with GDPR.
- Global Companies: Any company that markets goods and services to EU states and completes transactions with EU citizens and residents is also expected to maintain GDPR compliance, regardless of where the corporation is located. Even if they have no staff or equipment located in the EU, if their marketing efforts extend to the EU or they use personal data to track the behavior of EU citizens, they are subject to GDPR rules.

**Rights and requirements**

The key highlights of the GDPR include:

- **Privacy by design and default** – GDPR states that organizations must include privacy in their processes and systems by design. Privacy can no longer be an afterthought when developing new products, which must adhere to the tenets of the GDPR. For instance, a company’s software and systems should be capable of complete erasure of personal data if requested.

- **Right to be forgotten** – Organizations cannot hold any data without prior approvals and need to have strict mechanisms in place to delete data if requested by users, or data subjects.

- **Right to Data Portability** – GDPR allows data subjects to obtain and transfer personal data from one data controller to another, in a safe and secure fashion.

- **Explicit opt-in consent** – GDPR strengthens the case for explicit opt-in consent from customers before using their personal data. Under the regulation, the data subject is completely in control of their own data. Organizations also need to make sure they communicate clearly when asking for personal data and be clear about its intended use.

- **Significant non-compliance fines** – Article 79 of the regulation states that non-compliance will result in penalties of up to 4 percent of worldwide turnover or 20 million Euros, depending upon the nature of the violation.
• **Stricter rules for data breaches** - Breach notification is another key provision of GDPR. Under this provision, it will become mandatory for organizations to notify the data protection authority and its customers within 72 hours of a data breach.

• **Appointment of a Data Protection Officer (DPO)** for data controllers, with the responsibility to systematically review, assess and report on compliance when large-scale processing of PII occurs.

### Data Controllers and Processors

Both data processors as well as data controllers are liable under GDPR. A data controller is the entity that determines the purposes and means of processing of the personal data. (Article. 4 (7)). Controllers are the only entity with direct contact with the data subject.

A data processor is the entity that processes personal data on behalf of the controller. (Article. 4 (8). “Processing” refers to operations performed on personal data such as collection, structuring, storage, adaptation or alteration, retrieval, use, misuse, erasure or destruction. (Article. 4 (2)). Between the two should exist a binding contract, which establishes the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. (Article. 28 (3-4)).

The GDPR mandates that data controllers engage only data processors able to provide sufficient contractual guarantees and which have the capacity to comply with the GDPR when executing data processing activities on behalf of the data controller. The GDPR also requires data processors to guarantee adequate cybersecurity.

### What it all means for Communication Service Providers

Preserving the integrity and security of customer data is a mainstream issue for CSPs as they collect customer data to introduce customized services and improved customer experiences. Much of this customization relies on personal data - namely information that allows an individual to be identified, either directly or indirectly. What can be classified as an ‘identifier’ now includes online identifiers such as IP addresses and geo-location data.

With the escalating value of PII, CSPs are attractive targets for attackers seeking unlawful access to sensitive data. They can also be the subject of politically-motivated attacks and hacking by nation states. Furthermore, malicious actors can exploit CSP networks for secondary attacks to infiltrate other corporations. With large numbers of employees, CSPs must manage and record access to all types of sensitive information, including customer data, employee records, company financial information, Call Data Records (CDR) and Internet Traffic and Transaction Data (IPDR).

PII and other sensitive data exist in many locations, making it difficult to protect against all threats. The challenge is compounded by the adoption of trends such as mobility, cloud computing and the Internet of Things, all of which increase the opportunities for attack, exposing new vulnerabilities, and redefining the network perimeter.
Compounding the effect, CSPs now often make use of complex heterogeneous networks. These networks curate and transmit large volumes of high value data. CSPs can quite easily have tens of thousands of servers and networking devices managed by countless external and internal system administrators.

For example, mobile network operators continuously process data from base stations to provide communication and value-added services. Location data derived from base stations are subject to regulations pertaining to PII – “location data constitutes any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service”.

In addition, if a CSP offers a hybrid geolocation service, which is also based on the processing of other types of location data such as GPS or Wi-Fi, that activity qualifies as a public electronic communication service.

**CSPs are both controllers and processors**

CSPs are considered both data controllers and processors. Any business that transfers information for data warehousing, reporting and marketing purposes will now need to be ready to delete or ‘anonymize’ these data sets. In addition, CSPs will also need to ensure that they store and use consumer information only with explicit consent and when it is not easily linkable to a single individual. Businesses that need to store data for legitimate legal purposes will now need to separate this data from other systems so that this data is not accidentally processed for other purposes.

CSPs operating outside of the EU may also be considered data processors or data controllers. This can occur when a business customer uses the communications company’s products or services to collect, use and/or store personal data regarding EU customers or potential customers.

For instance, if a North American based business customer uses a North American based email service to communicate with customers or potential customers in the EU, that service — the US business customer who collects, uses and/or stores that personal data from EU residents — is considered a data controller under EU law. North American service providers who provide email or other communications products/services to its business customers communicating with EU residents constitute EU data processors.

**CSPs have extra responsibilities**

In addition to the GDPR, the EU issued a draft e-privacy regulation in January 2017. The new e-privacy regulation will take effect on the same day as the GDPR and applies to all digital communications companies (including CSPs). Like the new GDPR, the e-privacy regulation applies to non-EU providers of communication services used to communicate with EU residents, regardless of whether the services provided are paid for or free. The e-privacy regulation incorporates the penalties and fines of the GDPR.

The e-privacy regulation is more far-reaching than the GDPR and protects data of “legal persons” i.e., businesses and organizations, as well as “natural persons” located in the EU. It also creates new data rights for businesses and individuals not included in the GDPR legislation, such as the right to confidentiality of digital message content and metadata and the integrity of a user’s digital device. This extends data privacy obligations to all digital communication providers, that is, all digital communications including content and metadata must be kept confidential except with the user’s prior consent. These include:

- Email and webmail
- Voice over IP (VoIP)
- Text and instant messaging
• Mobile applications
• Over-the-top (OTT) communication applications like Facebook, What's App and Skype
• Internet of things (IoT) devices
• Public Wi-Fi
• Metadata, cookies, direct marketing, online marketing and other similar online actions and campaigns

**Multiple attack vectors – insiders, endpoints and networks**

With hundreds of applications handled by thousands of representatives with direct customer information, communication service providers have always faced insider threats and risks. Whether from inadvertent, malicious, or targeted attacks, insiders account for up to 70 percent of all cyber issues. With access to privileged credentials, and operating within a perimeter, insiders are increasingly the target for phishing campaigns. For instance, to exploit a mobile service provider, external actors will target employees who can provide access to subscriber and company data. If the target is an Internet service provider, the attackers will try to identify the employees who can enable network mapping and man-in-the-middle attacks.

The threat landscape is significant in today’s mobile connected world. Service providers must take steps to protect not just PII data inside their networks, but also the integrity of devices which connect to these networks. Every smart mobile device has at least one unique identifier – the MAC address. The device may have other unique identification numbers, added by the developer of the operating system. These identifiers may be transmitted and further processed in the context of geolocation services. It is a fact that the location of a device can be calculated precisely – for instance, to a residence or to an employer.

With repeated observations, it is possible to identify the owner of the device. Moreover, a mobile device compromised with malware may expose additional valuable PII including:

• Business e-mails with customer and employee data
• Business apps with business-sensitive information
• Wi-Fi passwords and VPNs
• Contact details of customers and employees

CSP networks themselves rely on signaling systems, such as System Signaling 7 (SS7) and Diameter, to interconnect global communication networks. These systems enable mobile and fixed network operators to set up and tear down calls, route text (SMS) messages, support inter-network connectivity and transparent roaming and provide per-session information such as caller ID. SS7 networks were originally designed to work with a small set of trusted operators and as a result, security was not a top design consideration, leaving CSPs open to attack. SS7 vulnerabilities can be exploited to illegally obtain access to a subscriber’s unique identifier and location, which is then used to facilitate other security attacks.

A provider’s Domain Name System (DNS) is another attack vector which could be targeted to obtain PII. CSPs must safeguard DNS’ against external threats and attempts to extract data.
Who is responsible for compliance?

Section 4 of GDPR mandates a statutory position of Data Protection Officer (DPO) who will have a key role in ensuring compliance with GDPR. A requirement to appoint a DPO applies to both controllers and processors. There is no exception for small or medium-sized companies, who can follow a risk-based approach to determine whether a DPO is required.

The GDPR requires the appointment of a DPO in the following cases:

- Public authorities or bodies (except courts)
- Private companies where the “core activities” consist of
  - Processing operations which require “regular and systematic monitoring” of data subjects “on a large scale”
  - “Large scale” processing of sensitive data

The definition of “large scale” depends on the number of data subjects (e.g. customers or subscribers) concerned, the volume of data and/or range of different data items, the duration or permanence of the processing and the geographical extent. Most, if not all, CSPs would be considered large-scale controllers and processors of PII.

Even where the GDPR does not specifically require the appointment of a DPO, it is highly encouraged by the European Article 29 Working Party (WP29) as a matter of good practice and to demonstrate compliance.

When GDPR is in effect, risk of non-compliance includes loss of goodwill and stiffer fines. In 2016, UK based mobile operator TalkTalk was fined for security failings that allowed hackers to access customer data. If GDPR had been in place, the penalty could have been as high as £59 million.

Get ready for GDPR

GDPR is a principle-based regulation - it specifies what to do, but not how to do it. In Article 32, Security of Processing, GDPR states that the Controller and the Processor shall implement appropriate technical and organizational measures to mitigate risk. Commonly in any organization, risk spans three broad categories: People, Data and Application, which are interconnected over Networks.

Identify where personally identifiable information (PII) data resides

Assess current data collection and storage practices to identify where PII is stored. This should include an understanding of the business requirements for retaining such data, including who has access to it and what data security controls (e.g., encryption) are in place. Organizations should aim to minimize their collection of PII data.

Implement controls to protect PII

Organizations should ensure the appropriate security controls are in place to secure and protect collected PII. Recommended approaches include strong access controls that limit data access to a need-only basis and encryption of data at rest or in-motion. Organizations should also assess the flow of data within and outside the organization and the security controls that protect against accidental data leakage due to insider threats, negligent employees, or data breaches and cyberattacks.
Update incident response processes

Organizations must ensure they have implemented an effective incident response plan specifically to deal with any type of data breach. This includes procedures for handling breach notifications as required by the GDPR, evidence collection and storage, continuing communication with the relevant authorities and reporting the breach to the data subject.

Conduct periodic reviews

Organizations must periodically assess procedures pertaining to the collection, analyses and storage of PII data to reduce risk and ensure compliance with GDPR. They must assess compliance and provide verifiable proof in the form of reports. Additionally, they must periodically test and validate the incident response plan to ensure roles and responsibilities are clearly understood and followed.

Implement Role-Based Access Control

Organizations should collect minimal PII data and limit access to authorized users. Access management controls, which include detection and auditing of privileged accounts that have access to the systems containing personal data, are essential for preparing for GDPR. Identity Access Management (IAM) solutions reduce the insider threats, eliminate the anonymity of the shared accounts, enhance accountability, provide an audit trail of user activity and provide an important cornerstone on which to build GDPR compliance. IAM is a security practice that ensures the right individuals have access to the right resources at the right time. It helps to protect data, applications and people at the same time and provides all the necessary reporting tools to contribute to demonstrating compliance.

A privileged identity management strategy will provide detailed, role-based access control capabilities, allowing organizations to restrict access to data based on business need, the identity profile of the user and the type of data being accessed. This is a key aspect of GDPR compliance. Privileges or limitations can be assigned to groups or individuals. Audit logging is a necessity for GDPR compliance. Any privileged identity access management system must log user activity.

Nokia NetGuard Security

Nokia NetGuard provides a portfolio of security products and professional services that can help communications service providers assess their GDPR readiness and implement appropriate measures to ensure continued compliance.

Individual NetGuard products are designed to meet specific requirements of the GDPR. These products are designed for specific areas of protection such as security management, network security and endpoint security.

A typical security management product is the Security Management Center that allows CSO and DPOs to measure, monitor and report on security risks and compliance.

Network security products include NetGuard Virtual Firewall, a next-generation cloud-native virtualized firewall, supporting industry leading hypervisors.

End point security includes NetGuard Certificate Manager. A trust-framework, NetGuard Certificate Manager enables bootstrapping of digital trust, providing identity credentials to (virtual) network elements, endpoints and applications.
Conclusion

As people spend more time online and exchange ever growing amounts of data with service providers and other organizations, the risk of data breaches causing harm and financial loss grows more acute. Trust between citizens as the providers of data and companies and official bodies as the users of that data, has never been more vital.

With the GDPR, the EU is attempting to enhance that trust by deepening and extending the rights of citizens to say how and when their personal data is used, as well as increasing the responsibilities of data users and processors to protect that data.

As organizations that constantly exchange data with their users and that build up huge amounts of information on the habits, locations and preferences of their subscribers, communications service providers are prime targets for people who would seek to gain from unauthorized access to this information.

The sensitive nature of this data is recognized by the EU, which has put in place regulations that go even beyond the stringent requirements of the GDPR itself.

As such, service providers need to put in place robust processes and solution that allow them to meet these obligations. Nokia NetGuard is a suite of solutions that allows providers to meet the requirements of each article of the GDPR, ensuring they can continue to safeguard their customers’ online life.