GDPR Reference

This article helps define in simpler language the most common GDPR terms and general provisions of the law to provide clearer understanding of the relationships between end users, customer organizations, and NocTel. Please carefully note **there is no standard interpretation** of terms and provisions of GDPR law, so the information captured here may change frequently after **May 25th, 2018**. When changes occur, generally expect to see changes elsewhere such as NocTel's Terms of Service and Privacy Policy.

> ⚠ This article does not constitute legal advice nor seeks to encourage or discourage customers and end users from seeking appropriate legal counsel. The information provided here is intended to build a basic understanding of GDPR law and is not comprehensive nor conclusive.

- GDPR Law Summary
- Key Terms
  - Data Subject
  - Personal Data
  - Data Controller
  - Data Processor
  - Data Protection Officer (DPO)
  - Data Rights
- Quick Bits and Questions
  - Who is covered under GDPR law?
  - What is "personal data" under GDPR? Is it different from PII?
  - Do all requests invoking personal data rights need to be accommodated?
  - Couldn't companies and services just block anyone from the EU from access?
- GDPR Related NocTel Specific Questions

GDPR Law Summary

GDPR - or the **General Data Protection Regulation** - is an EU law that will become enforceable worldwide as of **May 25th, 2018**. Its basic intent is to provide personal data protections and fundamental rights for end users who provide personal data to services, applications, and companies whether they are aware of the data collection and processing or not.

Key Terms

Data Subject

A data subject is an identifiable or identified *natural person*. A natural person here means an actual existing or having existed human being. It does not adopt the definition of "person" in the business law sense, so corporations are not qualified as data subjects under GDPR.

Personal Data

"Personal data" under GDPR is defined as:

*"**any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

In other words, it's almost anything relating to a *natural person* (see above) that can be used to identify them uniquely.

Personal data also defines a more restricted sub-classification known as *sensitive personal data*. Sensitive personal data is generally limited to one's biometric and genetic information as well as very personal details such as sexual orientation, political sentiment, and religious association.

Data Controller

Data controllers are defined as "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.*"

In other words, they are usually entities that are requesting personal data but may not be performing any of the collection, storage, or processing of the data. Data controllers will typically have some access to personal data that is collected, stored, and processed.

Data Processor

Following off the definition of a data controller, a data processor is defined as *"natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."*

In many cases, a data processor is a third party service provider of some variety to another company, service, or application. If your company uses

Data Protection Officer (DPO)

The ICO recognizes that some companies may be prone to misreport compliance activities if left to self-implement. To counteract this potential, the ICO introduces the station of Data Protection Officer who is generally responsible for the following:

- to inform and advise the organization and its employees about the obligation to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits
- to advise on, and to monitor, data protection impact assessments
- to cooperate with the supervisory authority
- to be the first point of contact for supervisory authorities and for data subjects
- to take into account the risk associated with the processing occurring with regard to the nature, scope, context and purposes of the processing
- to prioritize and focus on the more risky activities or where the potential impact on individuals could be damaging

Not every organization that acts as a data controller and/or data processor needs to instate a DPO, but generally these are the guidelines for when a DPO is necessary:

- your organization is a public authority
- your organization's normal operations require large scale, regular and systematic monitoring of individuals
- your organization's normal operations consist of large scale processing of special categories of data or data relating to criminal convictions and offenses

Unfortunately, where the line is drawn on what volume of processing of personal data constitutes "large scale" is highly subjective, but should be erred on the side of caution.

Data Rights

GDPR defines the following broad data rights of data subjects:

- **The right to be informed**: the right to be informed about the collection and use of personal data. This generally accommodated up front through privacy policies, explicit opt-in prompts, and notices within applications and services when it occurs. These notices must be provided in plain language and cannot be blanketed as a single, vague statement.
- **The right of access:** the right to receive confirmation personal data is being processed and access to personal data that is on record. There are some contentions involved with what format the personal data should be made available in for ease of understanding and completeness.
- **The right to rectification:** the right for data subjects to have inaccurate personal data corrected or completed if it is incomplete. Requests for rectification can be submitted verbally or in writing to the data controller or data processor where the data controller or data processor has at most one (1) calendar month to respond to the request. However, there are certain circumstances where rectification requests cannot be honored, such as if the data in question reflects an opinion rather than a fact. Often changing the record of such data retroactively changes circumstances in the larger context of the data in possibly significant ways.
- **The right to erasure:** also known as "the right to be forgotten" or "the right to be deleted." Such requests can be submitted verbally or in writing and the data controller and/or data processor has one (1) calendar month to respond. However, relative to how the personal data is processed, the data controller/data processor may have legitimate grounds to deny the request. General good practices stipulate personal data be deleted or sufficiently anonymized when the data subject no longer has business with the data controller/data processor, which signifies having no legitimate interest in maintaining or processing the data. Out of all the personal data rights, this right in particular is most challenging to accommodate for most organizations.
- **The right to restrict processing:** the right to request the restriction or suppression of personal data, but is *not* an absolute right and only applies to certain circumstances. Fulfillment of requests regarding this right only restrict personal data *processing* and not does not apply to the collection and storage of the personal data in question. Like several other rights, the right to restrict processing can be submitted verbally or in writing with one month to respond.
- **The right to data portability:** this allows data subjects to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way without affecting its usability. This only applies to information a data subject has provided to a controller.
- **The right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, direct marketing (including profiling), and for the purposes of scientific/historical research and statistics. This right is not absolute and can be overridden where there is sufficient legitimate reason to process the personal data, otherwise there is no reason to deny the request.

Bear in mind that while complaints and requests made invoking personal data rights under GDPR are generally accommodated, there do exist certain circumstances in which a data controller or processor can legitimately deny the complaint or request.

Quick Bits and Questions

Who is covered under GDPR law?

EU residents. Some contention in interpretation exists as to whether this means individuals physically residing in the EU or the individual in question is just an EU resident. This means the latter interpretation would require GDPR compliance by foreign companies who do any sort of business with EU residents, typically during travel or vacation. It's the safer bet to use the latter interpretation.

When the law talks of "EU residents" it means individuals and by "individual" that is restricted to *natural persons*. In other words, a real, live human being and not a "person" in the business law definition. This means corporations are not considered protected under GDPR.

What is "personal data" under GDPR? Is it different from PII?

Personal data in GDPR compared to PII (Personally Identifiable Information) is much more broad and includes types of data such as geo-coordinates provided by GPS and IP address. Personally Identifiable Information is generally a US-specific term and should not be thought of as equivalent to *personal data* in the context of GDPR.

Do all requests invoking personal data rights need to be accommodated?

Yes and no. It depends.

The ICO sets forth some guidelines of reasons why a company may decline to accommodate a request involving personal data rights. The most common reason is **legitimate use**, which can take precedence in retaining and otherwise processing personal data over some requests. Legitimate use also covers obligations to other compliances and protocols the company must observe. A less often feasible reason the ICO recognizes is if accommodation of the request shows a demonstrated exorbitant time, effort, and financial cost to service.

For example, if an employee is fired from a company after making repeated verbal threats to coworkers, the company may reasonably decline the former employee's request to the right to be forgotten. The company may partially accommodate this request by agreeing to not share the conditions of the employee's departure with others, but the company itself for its own records maintains the right to keep that data as it may include relevant information such as if the employee is eligible for rehire and what position they held prior to departure.

With few reasonable exceptions, companies are otherwise expected to accommodate personal data right requests from data subjects. Additionally, dependent on the type of request the company in question must accommodate the request with all reasonable haste.

Couldn't companies and services just block anyone from the EU from access?

Technically yes, but it's generally agreed this is not an effective solution to sidestep the need for GDPR compliance. The reason blocking access from the EU would be ineffective is it does not account for the use of VPNs and/or proxy servers to reach otherwise blocked sites and services. Additionally, with the vague interpretation in the law itself of what constitutes an EU resident, the case of EU residents traveling abroad and utilizing services in person such as banks, transportation services, lodging, etc. circumvents the "protection" of blocking outside access as the EU residents are physically located outside the EU.

Currently, there is no provision in the GDPR law which recognizes simply denying or blocking services to EU residents as a legitimate means of respecting and protecting personal data. Given this, it also does not recognize the case where an EU resident falsifies point of access and other personal data to access and utilize services that otherwise explicitly want to avoid EU residents.

GDPR Related NocTel Specific Questions

Is NocTel seeking GDPR compliance?

It's something that's very much on the radar, but various internal challenges exist that have caused efforts toward legitimate GDPR compliance to be slower than would be preferred. Until NocTel is able to attain GDPR compliance, we intend to make operations in relation to personal data and privacy as transparent and straightforward as possible so you know we're on the right track.

Given the size of NocTel and the vast majority of customer organizations not having normal contact with EU residents, NocTel at this time has determined it is not reasonable to instate a DPO.

Will NocTel process personal data requests that come from non-EU residents?

NocTel will do its best to treat all personal data requests equally as GDPR represents valuing and respecting personal data.

Can NocTel accommodate my personal data request directly?

While NocTel will exert due diligence to honor personal data requests that are determined to be valid, it is not recommended to submit these requests directly to NocTel. Our basis is our customers are organizations and subscribe to NocTel for business services. Accommodating any data requests without the awareness and agreement of the organization the requesting data subject is part of may cause disruption of services and manageability of the data subject by account administrators.

NocTel recommends that any personal data right related requests be submitted to your organization first and then is received by NocTel with the affirmation that some features and manageability could possibly change in relation to you.

What are examples of personal data requests NocTel will not accommodate?

Here are some examples and the reasoning why the request will not be accommodated:

- *Request to delete IP addresses and device MAC addresses associated with a data subject* (exercising right to be forgotten, right to restrict processing): Without the ability to collect and store hardware IP address and MAC address, NocTel's system has no way of accurately identifying or integrating the device. Accommodating this request would effectively cause all services to cease functioning for the data subject. This is additionally not tenable as the hardware and addresses in question typically are owned by the data subject's organization, not to the data subject themselves. While this is qualifies as personal data, the data subject is associated by virtue the resources have been assigned with the express purpose the data subject can fulfill their responsibilities to their organization.

- *Request to exclude data subject's handset usage and activities from logging and audit reports* (exercising right to restrict processing): NocTel cannot accommodate this request as the data subject in almost all cases uses NocTel's VoIP services to serve the interests of their organization. Therefore, activities performed within the system and in regard to usage are legitimate data NocTel has an obligation to provide to the customer organization.

- *Request access to data subject's personal data on record within NocTel's systems* (exercising right of access): This request should be submitted through the data subject's associated organization. NocTel's end user management via control panel *can* be setup such that a customer account's users all have access to their own extension and data. In many cases, customer organizations choose to only have NocTel control panel user accounts for IT technical and administrative staff who then manage all other end users in the organization. The relevant data in the request is reasonably accommodated through audit reports for the particular data subject.

- *Request to port all personal data out of NocTel with the intent to seek services with a different provider* (exercising right of portability): This request is something NocTel can only at best partially accommodate. Telecommunications is an industry in where the process of porting numbers between providers tends to be an extremely tedious process. For the act of porting numbers out of NocTel, the porting request needs to submitted to the new service provider who then submits the associated porting request information. If the porting request information is accurate, the number (s) are ported. If it's incorrect, the port will not occur. This porting process takes precedence over GDPR's right of portability as this process is standard in telecommunications. For portability, NocTel can provide a list of extensions and phone numbers, but cannot reasonably provide personal voicemails or faxes in a correlated output for what voicemail and fax data still exists in NocTel's system.

- *Request to restore deleted data:* In most cases this variety of request comes when an end user (data subject) deletes data such as voicemail recordings or received faxes. NocTel processes deletion of this data as absolute and cannot be undone. When a deletion occurs as triggered by an end user or automatic retention policy, there is no delay in the deletion of the data in question across the entire system. This means there is no window for recovery, so this particular request cannot be accommodated.

What is NocTel's policy for storing and processing personal data?

See our Privacy Policy for information on personal data retention.

Generally, NocTel only keeps personal data for as long as it's valid and needed. For example, a setting that stores personal data for a feature will overwrite and consequently forget the previous value if it changed. Likewise, for personal data such as voicemail, NocTel implements an automatic data retention policy that will delete old voicemails that have not already been deleted by the end user themselves.