GDPR: A Comprehensive Overview

Outline

① What is the GDPR and why do we have it?

② What are the major changes?

③ Where to report a breach?

④ Additional resources

1. What is the GDPR and why do we have it?

The general data protection regulation will go into force on May 25th, 2018 and extends the privacy rights of data subjects within the European Union.

The regulation applies to any data controllor or processor that is offering goods and services to people living in the EU. This includes refugees, people on work visas, etc.

1. What is the GDPR and why do we have it?

☞ Replaces the Data Protection Directive (1995)

> “Up to now, businesses in the EU had to deal with 28 different data protection laws. For many companies looking to access new markets, this fragmentation created costly administrative burdens.
>
> The same rules will apply both to companies established in the EU or outside the EU. All companies processing the personal data of individuals based in the EU offering services or products will have to comply with the EU data protection rules. [1]

[1] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business_en.pdf

1. What is the GDPR and why do we have it?

- ☞ Part of the strategy to achieve a single digital market

  “The Digital Single Market strategy wants to allow better access for consumers and business to online goods and services across Europe.[2]

  - ☞ Rules to make cross-border e-commerce easier
  - ☞ More efficient and affordable parcel delivery
  - ☞ Ending unjustified geo-blocking
  - ☞ A modern, more European copyright framework
  - ☞ Reducing VAT burdens

[2] https://ec.europa.eu/digital-single-market/en/better-access-consumers-and-business-online-goods

2. What are the major changes?

Core Principles:[3]

① **Transparency**. Personal data must be processed lawfully, fairly, and transparently

② **Legitimate Purpose**. Personal data can only be collected for specified, explicit and legitimate purposes (purpose limitation)

③ **Data Minimisation**. Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

④ **Data Accuracy**. Personal data must be accurate and kept up to date

⑤ **Data storage limitation**. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing (storage limitation)

⑥ **Data confidentiality and security**. Personal data must be processed in a matter that ensures its security (integrity and confidentiality)

[3] https://gdpr-info.eu/chapter-2/

2. What are the major changes?

- ☞ The data controller is responsible for breaches happening at the data processor
- ☞ New fines up to 4% of annual revenue or 20 million whichever is higher

2. What are the major changes?

The right to know who is processing what, and why

Bought something online?

The seller must collect only the data needed to fulfil the contract. They must also provide you with the information listed above, and delete the data when they no longer need it.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to access your data

Apps asking too much?

You bought a fitness tracker and subscribed to a health app that monitors your activity. You can ask the app operator for all the information processed on you. This includes all subscription data (such as your name and contact details where relevant) and all information collected about you through the tracker (such as heart rate, performance, etc.).[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to object

Fed up of ads?

You bought two tickets online to see your favourite band play live. Afterwards, you're bombarded with adverts for concerts and events that you're not interested in. You inform the online ticketing company that you don't want to receive further advertising material. The company should stop processing your data for direct marketing and, shortly afterwards, you should no longer receive emails from them. They shouldn't charge you for this.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to correct your data

Incorrect data costing you?

You apply for a new insurance policy but notice the company mistakenly records you as a smoker, increasing your life insurance payments. You have the right to contact them and get this corrected.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to have data deleted and to be forgotten

Search results irrelevant?

When you type your name into an online search engine, the results include links to an old newspaper article about a debt you paid long ago. If you're not a public figure and your interest in removing the article outweighs the general public's interest in accessing the information, the search engine is obliged to delete the links.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to have a say when decisions are automated

Applying for a loan?

You apply for a loan with an online bank. You are asked to insert your data and the bank's algorithm tells you whether the bank will grant you the loan and gives the suggested interest rate. You must be informed that you may: express your opinion; contest the decision; and ask for a person's input in the process to review the algorithm's decision.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

The right to move your data

Found a cheaper supplier?

You've found a cheaper electricity supplier. You can ask your existing supplier to transmit your data directly to the new supplier, if it's technically feasible. In any case, they must return your data to you in a commonly-used and machine readable format so that it can be used on other systems.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

2. What are the major changes?

Data lost or stolen?

The rules make sure you are protected. The organisation holding your data has to inform the national Data Protection Authority if the data breach is a risk. If the leak poses a high risk to you then you must also be informed personally.[4]

[4] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf

3. Where to report a breach?

“Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).[5]”

[5] GDPR Article 51(1) https://gdpr-info.eu/art-51-gdpr/

3. Where to report a breach?

Ms. Andrea Voßhoff

Bundesbeauftragte für Datenschutz und Informationsfreiheit

poststelle@bfdi.bund.de
+49 (0)228-997799-0[6]

[6] https://www.bfdi.bund.de/DE/Service/Kontakt/kontakt_node.html

4. Additional resources

- ☞ https://gdprchecklist.io/
- ☞ https://techblog.bozho.net/gdpr-practical-guide-developers/
- ☞ https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis/
- ☞ List of data protection authorities: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

Thank You