How to ensure **GDPR compliance** for your **startup**

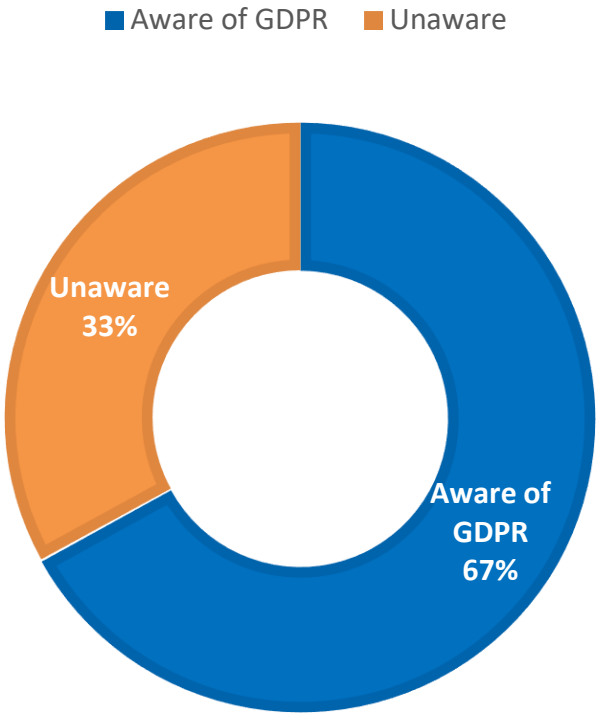
presented by **Ray Migge | corum Rechtsanwälte**

Goals of GDPR

1. protecting the rights of users
2. ensuring that data privacy laws keep up
3. creating unified and consistent legislation

GDPR statistics 2019

67 % OF PEOPLE HAVE HEARD OF GDPR AND ARE AWARE OF IT.



57 % KNOW THAT THERE IS AN AUTHORITY PROTECTING RIGHTS

Fines

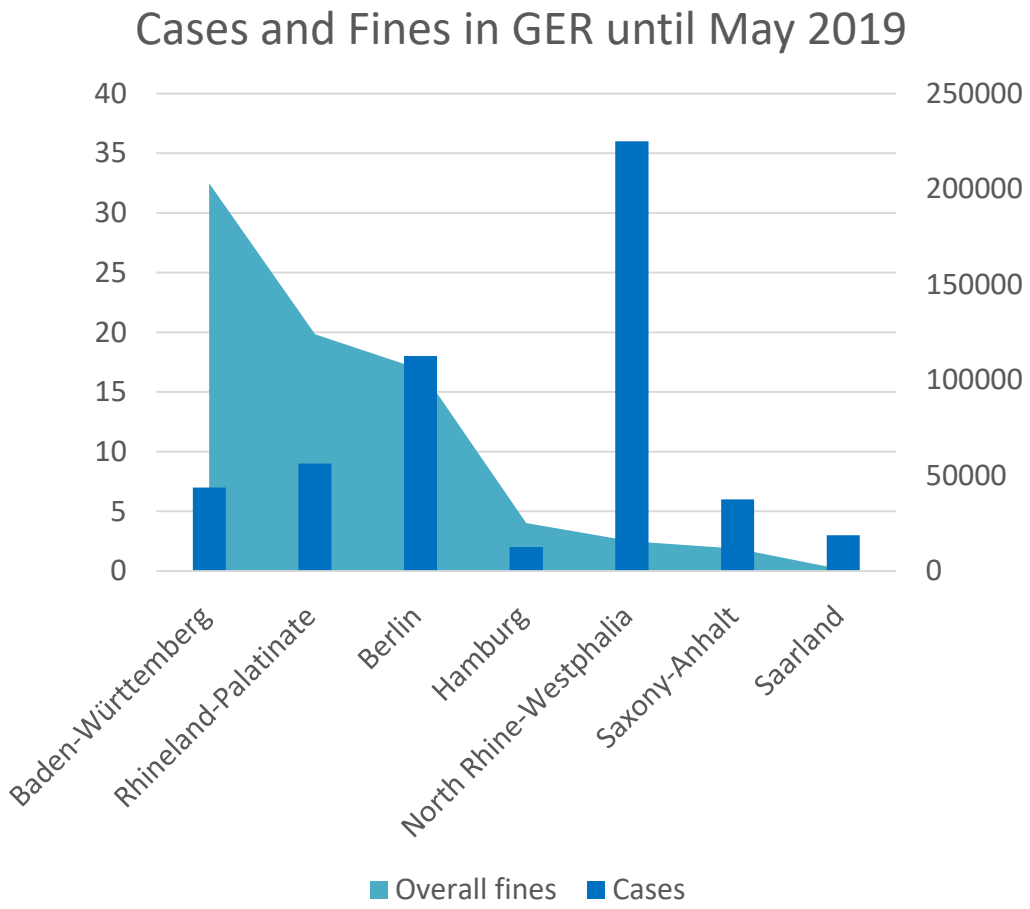
- Fine range per Art. 83 (4) GDPR
  - 10 million EUR or
  - 2 percent of the worldwide annual turnover
- Applicable areas of infringement:
  - conditions for children's consent
  - processing that doesn't require identification
  - general obligations of processors and controllers
  - certification
  - certification bodies

- Fine range per Art. 83 (5) GDPR
  - 20 million EUR or
  - 4 percent of the worldwide annual turnover
- Applicable areas of infringement:
  - data processing principles
  - lawfulness of processing
  - conditions for consent
  - processing of special categories of data
  - data subjects' rights
  - data transfers to third countries / int. org.

Highest fines in EU

Country	Institution	Fine
United Kingdom	British Airways	204,600,000
United Kingdom	Marriott	110,390,200
France	Google Inc.	50,000,000
Austria	Austrian Post	18,000,000
Germany	Deutsche Wohnen	14,500,000
Bulgaria	National Revenue Agency	2,600,000
Netherlands	UWV (insurance service provider)	900,000
Poland	Morele.net	645,000
Bulgaria	DSK Bank	511,000
France	Futura Internationale	500,000
Netherlands	Haga Hospital	460,000
France	SERGIC (Real Estate)	400,000
Portugal	Public Hospital	400,000

Fines in Germany



- Largest fines in Germany:
  - Deutsche Wohnen: 14,500,000 EUR
  - Delivery Hero: 195,407 EUR
  - N26: 50,000 EUR

Applicability

- The GDPR applies to
  - “data controller”
    - a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
    - a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU;
    - i.e. the “data controller”.
  - “personal data”
    - any information relating to an identified or identifiable natural person

Principles of GDPR

- Legality and transparency
- Specified, explicit and legitimate purposes
- Data minimization
- Correctness
- Storage limitation
- Integrity and confidentiality
- Accountability

Measures

Record of Processing Activities - Burden and Chance!

- Required for every company controlling or processing personal data (Art. 30 GDPR)
- Written directory (a table is sufficient):
  - which data is collected,
  - when,
  - how, and
  - why,
  - who can access it, and
  - how the data subject has consented.
- Important: In addition to customer data, internal data such as staff data or payroll accounting data must also be included.

Data Flow Chart – Know your processes!

- Not required, but useful
- Shows the flow of data between all relevant parties in your business model
- Helpful to detect weak spots or identify third parties with access to data

Data Protection Officer – Seek Help!

- Required when
  - (a) public authority, (b) processing on large scale or (c) processing of special personal data on large scale
  - per BDSG also when 20 employees
- DPOs
  - assist in monitoring internal compliance
  - inform and advise on data protection obligations
  - provide advice regarding Data Protection Impact Assessments (DPIAs)
  - act as a contact point for data subjects and the supervisory authority.
- DPO must be
  - independent,
  - expert in data protection,
  - adequately resourced, and
  - report to the highest management level.
- DPO can be an existing employee or externally appointed.

Technical & Organizational Measures – Data security!

- Art. 32 GDPR list is not obligatory, but indicative of the standard:
  - Most obvious:
    - pseudonymization and encryption;
    - ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services
- concrete measures for data security determined individually for each company
- scope of the precautions depends on the
  - sensitivity of the data, and
  - probability of an attack
- Most obvious measures:
  - encrypt communication (problem: e-mail)
  - protect access to personal data with personalized passwords
  - set up virus program and firewall
  - data processing agreement

Compliance on Websites

- Privacy Policy
- Cookies
  - List of cookies
  - Cookie notification
- User request forms
- Other forms
  - Add checkboxes and link to Privacy Poliy
- Plugins and applications
  - Ensure GDPR compliance or switch
  - List in privacy policy
  - Possible data processing agreement necessary
- CMS
  - Update to GDPR compliant versions
- Checkout pages
  - Add checkboxes and link to Privacy Poliy
- Email notification
  - Only use double opt-in, delete all other data
  - Provide easy unsubscribe method
- Backups
  - Ensure security of backups
- User request response
  - Ensure reply within 2 days
  - Deletion, update, provision of data within 30 days
- Opt-ins
  - Remove automatic opt-ins

Privacy Policy – Inform your Customers/Employees!

- Required as soon as personal data is collected or processed (including IP address)
- Informs about the type, scope and purpose of the collection and use of personal data
- Top priority is comprehensibility and transparency
- Language of the addressee, on websites accessible from every page
- Must contain at least
  - Contact details of the controller/processor
  - Purposes for which personal data is processed
  - Legal basis for data processing
  - Data storage time
  - Rights of data subjects

Important: non-exhaustive list!

Data Protection Impact Assessment!

- Required in cases of high risk for personal data
  - systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
  - a systematic monitoring of a publicly accessible area on a large scale
- Prior to processing
- Must include at least:
  - systematic description of operations, purposes and interests
  - assessment of neccessity
  - assessment of risks to rights and freedoms of data subject
  - measures to address risks

Training, Compliance Commitment and Documentation

- Train your employees!
  - Authorities suggest written commitment by employees to comply with data protection
  - Should be preceded by written explanation of GDPR and processes
- Documentation of all measures, assessments and activities

Process Manual – Make it easy for yourself!

- Definition of all processes associated with data processing
- Provides yourself and employees with information on how personal data is processed in order to avoid errors.
- E.g.
  - What is the process when a customer insists that his data be deleted? Who is responsible for this?
  - What is the process if there is a data leak and personal data falls into the wrong hands?
    - i.e. duty to report to the authorities and possibly to the data subject within 72 hours

Summary

- GDPR provides an opportunity for businesses and customers!
- Good preparation and a strategic approach will lead to success!
- Use checklists to address GDPR.

Thank you for your attention

Contact me at any time:

Ray Migge | migge@corum-pg.de | 0211 324 024

corum Rechtsanwälte – Elisabethstr. 16 – 40217 Düsseldorf – www.corum-pg.de