Morgan Lewis

TECHNOLOGY MAY-RATHON

The GDPR One Year On – a European and US review

May 22, 2019

Pulina Whitaker
Ezra Church
Charles Dauthier
Michael Junge
Axel Spies

The GDPR – Key Changes

- Data subject rights of access and rights to restrict or erase data and rights of portability – within one month (or up to three months); no fee
- Stricter processing requirements for special categories of data e.g. health information or biometrics:
  - express, informed, freely given consent
  - employment laws
  - assessment of working capacity
- Data protection impact assessment: required prior to processing if high risk for individuals

The GDPR – Key Changes

- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000 (depends on nature and extent of breach)
- Controllers and processors directly liable under GDPR
- Processor audit rights required by controllers
- Record keeping requirements
- DPO
- Appointed representative

Hot GDPR Issues

- Privacy notices – are they accurate? How to make them more understandable and transparent?
- Cookie notices – express consent?
- Data subject rights:
  - one month to respond – how to extend to three months?
  - dispute context – what is reasonable to withhold?
  - charging a fee or refusing to respond
  - managing supervisory authority investigations
  - redactions and exemptions

Hot GDPR Issues

- Data breaches:
  - investigations
  - vicarious liability?
- Solicitation of employees/customers or taking confidential information:
  - breach of restrictive covenants, contractual obligations, duties of fidelity or fiduciary obligations
  - separate data controller status
  - breach of local laws – criminal liability?
- New European consumer collective representations directive – privacy class actions?

Privacy Notices

Art. 12 (1) GDPR: *The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 […] in a concise, transparent, intelligible and easily accessible form, using clear and plain language […]. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means*; […]

- Most of companies have now adopted informative data privacy policies, with a few noticeable exception
- Having a privacy notice in place is however not a guarantee not to be sanctioned by data protection authorities for failure to comply with Articles 12, 13 and/or 14 GDPR:
  - Personal Data Protection Office (UODO) in Poland imposed, on 26 March 2019, a fine of €220,000 to a Polish company for non-compliance with Article 14 (3) GDPR

Privacy Notices

Privacy notice form and content imposed by the GDPR and data protection authorities have brought negative consequences:

- Privacy notices are long documents:
  - Mandatory to provide a single document easily accessible The mass of information is significant
  - Consequence: standard users will generally not read the privacy notice, whereas it was one of the primary goal of the GDPR.
- Content of privacy notices is very technical:
  - Main consequence for users: hard to understand, cause a frustration
  - Main consequence for companies: necessity to use services of a data privacy specialist to draft their privacy notice.
- Clarification on how to obtain user consent when required

Cookies - Consent

- UK requirements for GDPR standard of consent
- PECR – still not finalised
- Bavarian authority investigation
- AG opinion in *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*

Data Subject Requests

- The GDPR allows data subjects to exercise their privacy rights
- Controllers must:
  - respond to request within one month of receipt of the request
  - extend time period by up to two further months where appropriate taking into account "*complexity and number of requests*" - inform requestor within first month with reasons
  - right to refuse to respond if request is "*manifestly unfounded or excessive"*
  - no fee - unless request is "*manifestly unfounded or excessive*"
  - can charge a reasonable fee for copies
  - provide the information in a commonly used electronic format if the request is made by email
  - also provide summary of data processing information

The Right of Access

- The right of access is limited to information about the processing (similar to a privacy notice) and to a copy of the data subject's personal data
- No right to underlying documents
- First copy for free; administrative charge could be levied for further copies
- Need to redact other data subjects' identifying information
- Exemptions apply under local laws, e.g. under UK DPA 2018:
  - legal privilege
  - management forecasting
  - confidential references
- Take a proportionate approach and exclude:
  - administrative emails
  - emails copying in requestor

The Right to be Forgotten

- The right to erasure applies in limited circumstances:
  - the personal data is no longer necessary for the purpose the data controller collected it for
  - the data subject withdrew consent (where provided) and no other legal grounds for processing applies
  - the data subject objects to processing and there are no compelling legitimate grounds to continue processing the data
  - the data controller unlawfully processed the personal data
  - EU or member state law requires controller to erase the data
  - the data controller collected the personal data in the context of offering online services to children

The Right to be Forgotten (cont'd)

- Controllers can refuse to delete data where it is processed to:
  - exercise the right of freedom of expression and information
  - comply with a legal obligation under EU or member state law
  - perform a task carried out in the public interest
  - exercise official authority vested in the data controller
  - public health reasons consistent with the exceptions for processing special categories of personal data (such as health information)
  - archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, under certain circumstances
  - establish, exercise, or defend legal claims
- If the data controller made the personal data public, it must also take reasonable steps to inform other data controllers that are processing the personal data about the data subject's erasure request
- Liaise with data processors to implement the request

The challenge: How to make GDPR-policies more transparent and understandable….

Art. 5 (1) GDPR: *Personal data shall be: […] processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

- But observation after one year GDPR: Policies have become longer and longer ("document, document, document"). Negative consequences:

→ User: "I need a law degree to understand what this policy says…"

→ "Click fatigue", e.g. for cookie banners.

→ Some companies try hide problematic data processing in policies

→ Use of hyperlinks within a policy.

European consumer advocates (German VZBV etc.) are on alert.

A Big Task: How to Enhance Transparency

- German Interior Ministry (BTDrs 19/9186) recently suggested…
  - **Pictograms & icons** in the privacy statements "are well suited to provide users with better understandability of privacy policies."
  - **One Pagers:** Use of programs that "automatically read the privacy statements and point to certain aspects (e.g- data processing based on consent, tracking, data transfer to third parties) - see project "Privacy Guard.".
  - A "**legally compliant Europe-wide uniform model privacy policy**."
- Icons endorsed by EU Commission's GDPR Guidance: "Better rules for small business" https://ec.europa.eu/justice/smedataprotect/index_en.htm
- Recital 166 GDPR: The Member States should issue "*in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons*."

Examples of icons used in the EC's guidance

→No icon has been approved yet in Europe.

→The risk that an icon is misleading is on the controller.

GDPR in the US—Does it Apply?

- Does it apply?
- The GDPR applies to processors and controllers having an EU-based establishment where personal data are processed in the context of the activities of this establishment
- The GDPR also applies to controllers and processors based outside of the EU territory where the processing of personal data regarding EU data subjects relates to:
  - the offering of goods or services (regardless of payment)
  - the monitoring of data subjects' behavior within the EU

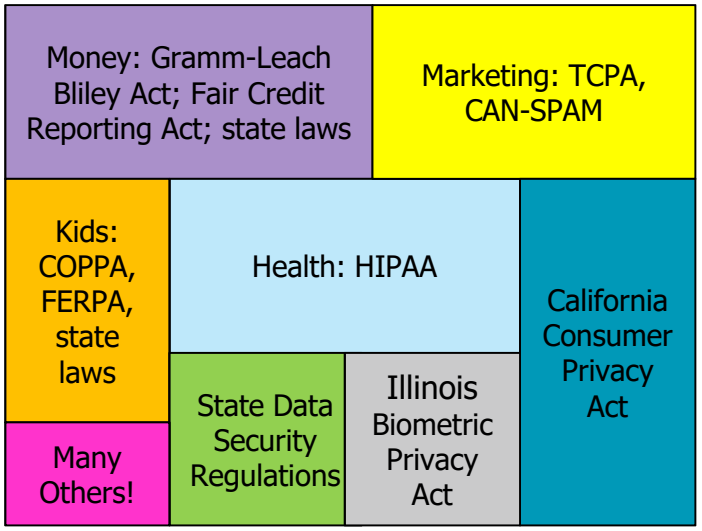
GDPR Challenges for US Companies

Comprehensive v. sector-specific.

GDPR

- One comprehensive privacy law
- All industries
- All personal data, regardless of type or context

US Privacy law



GDPR in the US—Trouble Areas

- Right to be forgotten
- Retention periods--no longer than needed for the purpose collected
- Breach reporting period
- Vendor contracts
- Data transfer

Passwords

According to Art. 32 GDPR "…the controller and processor shall implement appropriate technical …. measures to ensure a level of security appropriate to the risk, …."

The controlling of the implementation of these measures falls within the powers of the Data Protection Authority (Art. 58 GDPR) and a breach is subject to a fine of up to EUR 10 mio. or 2 % of the annual revenue (Art. 83 paragraph 4)

- **In 2018, the Data Protection Authority of the state of Baden-Wuerttemberg imposed a fine of EUR 20,000 for a breach of security by a social media provider. More than 1 mio. passwords were stored unencrypted and were hacked.**
- **Inspection of 20 websites (online shops, streaming portals, social media) by the Bavarian Data Protection Authority (DPA) in 2019 on security on the internet:**

Passwords

1) Does the service provider give guidance on a strong password?
   - 75 % of the investigated websites provide insufficient information.

2) How many characters do the service providers require?
   - The DPA recommends 12 characters. But 45 % of the service providers require only 8 characters and one website only even 4.

3) Does the website enforce a strong password?
   - None of the inspected service providers enforces a strong password. (Accepted weak passwords in the test: 0000; 123456; password; abcdefgh; ABC123)

Passwords

4) Does the website offer multi-factor authentication?
   - Multi-factor authentication, e.g. by SMS-code, app token or device identification, is recommended. 80 % of the websites offer password authentication only.
5) Is the email address confirmed after registration?
   - This practice is recommended to prevent criminals from logging in.
   - Only 25 % of the service providers send email address confirmation.
6) Are users warned of phishing risks during or after registration?
   - None of the websites provides sufficient information.(Information only given under FAQ or provided with fallacious authenticity tests, e.g. user informed that links starting with “https” indicate authentic emails from the service provider, but phishing mails can also show this characteristic.)

Passwords

7) Is the user informed about failed logins?
   - User should know if his "digital identity" is threatened.
   - Only 1 website notifies users of failed logins.

8) Change of password

Is the old password required for a password change?
   - 15 % of websites allow change of password during an ongoing session without entry of old password

Is the user informed about a password change?
   - Only 50 % of the inspected websites send such an information

Passwords

9) Does the service provider offer support for security requests and hacking?

- This is an indication whether a service provider really takes the protection of the user's data seriously.
- Only 6 of 20 websites offer such support.

As a consequence of these sobering results, the Bavarian DPA will contact the service providers and start further investigations.

Morgan Lewis Technology May-rathon 2019

A full listing and of our tech May-rathon programs can be found at

https://www.morganlewis.com/topics/technology-may-rathon

Please be sure to tweet **#TechMayRathon**

Thank you.

Pulina Whitaker

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses both labor and employment matters as well as data privacy and cybersecurity. She manages employment and data privacy issues in sales and acquisitions, commercial outsourcings, and restructurings. Pulina provides day-to-day advisory support for multinationals on all employment issues, including the UK's Modern Slavery Act and gender pay reporting requirements. She also advises on the full spectrum of data privacy issues, including preparing for the General Data Protection Regulation. Pulina has deep experience managing international employee misconduct investigations and has been appointed as a Compliance Monitor for a transnational organization.

Ezra D. Church

Ezra D. Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church focuses his practice on class action lawsuits and complex commercial and product-related litigation, with particular emphasis on the unique issues facing retail, ecommerce, and other consumer-facing companies. Ezra also focuses on privacy and data security matters, and regularly advises and represents clients in connection with these issues. He is co-chair of Morgan Lewis's Class Action Working Group.

Ezra has extensive experience handling complex and unusual class action litigation, and has handled all aspects of such cases from inception through trial and appeal. His work in this area includes defeat of class certification in a rare copyright class action against one of the world's leading publishers, successful opposition of class certification in an unusual defendant class action against many large financial institutions, and a successful defense verdict in a consumer class action trial against an international retailer, including affirmance on appeal. He is an active member of the Firm's Class Action Working Group and regularly writes and speaks on class action issues. He is a contributor to the Firm's chapter on class action litigation in the leading treatise Business and Commercial Litigation in Federal Courts and co-author of a chapter in A Practitioner's Guide to Class Actions, among others.

Charles Dauthier

Charles Dauthier
Paris
+33.1.53.30.44.74
charles.dauthier@morganlewis.com

Charles Dauthier advises French and international clients on both labor and employment matters, as well as data privacy and cybersecurity. He advises clients on executive terminations, collective terminations and other employment matters, as well as data privacy issues that surface in mergers and acquisitions, restructuring and outsourcing, and other types of reorganization. He counsels clients on employment matters attendant in employee benefits and employee representation matters.

Charles works with clients to comply with the General Data Protection Regulation (GDPR) and helps them manage employee misconduct investigations.. Prior to joining Morgan Lewis, Charles was an associate at another international law firm. His native language is French and he is fluent in English.

Michael Junge

Michael Junge
Frankfurt
+49.69.714.00.719
michael.junge@morganlewis.com

Michael Junge focuses on corporate, information technology, and data protection law, with a particular emphasis on advising companies on corporate governance. He has more than 20 years of experience working in the information technology sector, and has handled several large merger and acquisition transactions within the sector, including six multibillion-dollar take-overs, five of which were listed.

Before joining Morgan Lewis, Michael was group general counsel of a German blue chip company listed at the Frankfurt Stock Exchange and New York Stock Exchange. He has a strong foundation in capital market law and has had extensive dealings with regulators in Germany, Belgium, and the United States. Michael has a solid understanding of business processes and structures, including transformation and change management, and he served as a close advisor to a former member of the Commission of the German Corporate Governance Code.

Dr. Axel Spies

Dr. Axel Spies
Rechtsanwalt, Special Legal Consultant
Washington, DC
T +1.202.739.6145
E axel.spies@morganlewis.com

Dr. Axel Spies has advised clients for many years on various international issues, including telecommunications licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection, international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and equity purchases. A member of the Sedona Conference on Electronic Discovery, Dr. Spies is frequently quoted in the media for his telecommunications and privacy knowledge. He is also a co-publisher and frequent contributor to the German journals ZD (Zeitschrift für Datenschutz) and MMR (Multimedia Law) and a co-author of two German handbooks for companies on the GDPR.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.