Overview Recent GDPR Decisions, Lawsuits, Complaints, Fines and Guidelines[i]

I. Judgments

Jehovah's Witnesses (10 July 2018)

- *Background*: The case is about Jehovah's Witnesses Community and whether taking notes in the course of their door-to-door preaching falls under the GDPR.
- The European Court of Justice (ECJ) states that (a) their activities don't fall under the exemptions for religious communities, and that (b) the community is a data controller jointly with its members who engage in this preaching activity.
- Practical consequences: The status of a (joint) controller does not require that the controller has data access
- http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=524772

Internet Corporation for Assigned Names and Numbers (ICANN) v. EPAG Domainservices GmbH (EPAG) (30 May 2018)

- *Background*: EPAG wanted to sell domain names without collecting the domain owners' administrative and technical contact details, because it feared doing so would put it at risk of ruinous fines if it ran afoul of GDPR. However, its registrar contract with ICANN requires it to collect this information for the latter's global Whois system. To force it to comply with its contract, and to hell with GDPR, ICANN took EPAG to court in May, seeking an order banning the registrar from peddling domain names, if it refused to gather data for Whois.
- The Regional Court in Bonn rejected ICANN's initial application for an injunction, in which ICANN sought to require EPAG to collect administrative contact and technical contact data for new domain name registrations.
- https://www.icann.org/resources/pages/litigation-icann-v-epag-2018-05-25-en

The following judgments refer to directives that are no longer in force. However, the judgements were made with regard to the GDPR:

Independent Centre for Privacy Protection Schleswig-Holstein Germany (ULD) v. Schleswig-Holstein Business Academy (5 June 2018)

- *Background*: Schleswig-Holstein Business Academy operates a Facebook fan page and was ordered by the Schleswig-Holstein Data Protection Authority to deactivate the fan page. Neither Facebook Ireland Ltd nor Schleswig-Holstein Business Academy had been informing visitors of the functioning of cookies and subsequent processing of their data. The Business Academy took this case to court, arguing essentially that it was not responsible for the processing of data by Facebook or cookies installed by Facebook.

- The ECJ ruled that the operator of a fan page hosted on a social network must be considered a "data controller".

- http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=296736

Datenschutzbehörde Baden-Württemberg v. a Credit Agency (6 July 2017)

- *Background*: On 25 November 2016, the Data Protection Authority of the state of Baden-Württemberg ("DPA") imposed an administrative order on a credit agency, concerning an infringement of the GDPR. The DPA referred to future violations of the GDPR that the DPA expected to occur after 24 May 2018, as the legal framework will change. Under Recital 39 of the GDPR, controllers are obligated to establish time limits for erasure or for a periodic review. According to the order issued by the DPA, the credit agency must erase the stored data, after 24 May 2018, after the expiry of three years at the latest, beginning with the due date of the claim, except for the insolvency or unwillingness of the data subject to pay.

- The Administrative Court Karlsruhe held that there was no legal basis for the administrative order by the DPA. Both the GDPR and the current FDPA do not empower authorities to issue an order based on future violations of the GDPR before the GDPR applies

- https://www.delegedata.de/wp-content/uploads/2017/08/VG-Karlsruhe-10-K-7698-16u.pdf

II. Lawsuits

NOYB v. Google (Android)

- When the data subject activated a new Android phone for the first time he was forced to "agree" to the privacy policy and the terms. There was no option to use the phone without consenting.

- The consent is not freely given, as clarified in Article 4(11) of the GDPR and further specified in Article 7(4).

- The possible maximum fine under Article 83(5)(a), based on 4% of the worldwide revenue, would accordingly be about € 3.79 billion.

- https://noyb.eu/wp-content/uploads/2018/05/complaint-android.pdf

NOYB v. Facebook (Instagram)

- The wording "Agree to terms" is the only real option within the app to force data subjects to consent to the privacy policy. Only a small hidden link which says "See other options" seems like a potential way out. These options are however only the deletion of the users' account.

- The consent is not freely given, as clarified in Article 4(11) of the GDPR and further specified in Article 7(4).

- The possible maximum fine under Article 83(5)(a), based on 4% of the worldwide revenue, would accordingly be about € 1.3 billion.

- https://noyb.eu/wp-content/uploads/2018/05/complaint-instagram.pdf

NOYB v. Whatsapp

- In any case, the controller required the data subject to “agree” to the entire privacy policy and the terms.

- In addition to the forced consent to the privacy policy, the controller apparently attempts to “hide” consent to processing operations in the civil-law terms and seems to have the misguided view that these processing operations would then fall under Article 6(1)(b) of GDRP.

- The ‘core’ element of consent is the fact that it must be freely given, as clarified in Article 4(11) of the GDPR and further specified in Article 7(4) GDPR. A main objective of the GDPR was to stop frivolous gathering of consent in all shapes and forms. Thus, this complaint focuses primarily on the act of consent, which, in the present case, we do not see as “free”.

- https://noyb.eu/wp-content/uploads/2018/05/complaint-whatsapp.pdf

III. Complaints

Data breach complaints in the UK have risen 160% since GDPR came into force

- According to the Information Commissioner’s Office (ICO) complaints about potential data breaches have more than doubled since the General Data Protection Regulation (GDPR) came into effect.

- There were 6,281 complaints between May 25 2018, when GDPR came into force, and 3 July 2018, a 160% rise from just 2,417 complaints over the same period in 2017.

- https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf

France has registered an increase of more than 100% complaints since GDPR came into force

- Between 25 May and 1 October, the CNIL received 742 notifications of violations concerning data breaches, availability and integrity.
- More then half of the reported violations originate from hacking, malware or phishing.
- https://www.cnil.fr/fr/violations-de-donnees-personnelles-1er-bilan-apres-lentree-en-application-du-rgpd

On May 28, a French Digital Rights organisation called "La Quadrature du Net" has filed collective complaints against Google (Gmail, Youtube), Apple, Facebook, Amazon and Linkedin owned by Microsoft (People vs GAFAM).

- The complaints focus in the issue of "forced consent"
- The association is planning to bring action also against: Android, Whatsapp, Instagram, Skype and Outlook.
- https://vaaju.com/morroco/the-number-of-complaints-to-cnil-has-exploded/
- https://www.laquadrature.net/2018/05/28/depot_plainte_gafam/

Several complaints to the Data Protection Authority of the Republic of Austria:

- Violation of the right of access by the data subject (art. 15 GDPR)
  - The respondent is instructed to provide the information.
  - GZ: DSB-D122.844/006-DSB/2018
- Violation of the principles relating to processing of personal data (art. 5 para. 1 lit. e GDPR)
  - The respondent is instructed: a) to limit the storage of the respondent's master data to a maximum period of seven years; b) to delete the respondent's traffic data; c) to delete all personal data of the respondent which are not master or traffic data.
  - GZ: DSB-D216.471/0001-DSB/2018

- Violation of the right to erasure – 'right to be forgotten' (art. 17 GDPR)
  - The respondent is instructed to comply with the complainant's request for deletion of all data without delay, but at the latest within two weeks, and to subsequently inform the complainant in writing of the deletion of his data.
  - GZ: DSB-D216.580/0002-DSB/2018
- Compliance of the obligation to pseudonymise and encrypt personal data, art. 32 (1) a GDPR – Security of personal data
  - The court found that even though the controller omitted pseudonymisation, it can only determine a violation of the fundamental right to confidentiality ex post. The data subject cannot demand specific measures to minimize data within the meaning of Art. 5 (1) lit. c GDPR.
  - GZ: DSB-D123.070/0005-DSB/2018

IV. Fines

ICO fined AggregateIQ with £17 million for breaching GDPR regulations

- AIQ used algorithms from Facebook data held by CA (Cambridge Analytica) to build software to target Republican voters in the 2016 US election and,
- Worked to profile and target voters during the Brexit campaign
- The activity of AIQ continued even after the 25th of May, therefore GDPR rules are applicable.
- https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf

Non-Compliance of art 32 (1) lit.a GDPR – Security of personal data

- The State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg (LfDI) fined a social media company with €20.000 for not implementing appropriate technical and organizational measures, such as pseudonymisation and encryption of personal data
- The company had notified the supervisory authority following a data breach in which aprox. 330.000 email addresses and passwords were stolen.
- https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/

The Portuguese Data Protection Authority (CNPD) fined Barreiro Hospital with €400.000 for Non-compliance to GDRP and granting access to unauthorized personnel

- A £300.000 fine was applied for failing to respect patient confidentiality, and limiting inappropriate access to patient data
- The second fine is of £100.000 because they have failed to ensure the integrity of data security in their system
- The hospital filed for appeal

The Austrian Data Protection Authority (DSB) issued the first GDPR fine - €4.800 for large scale of monitoring public spaces

- An entrepreneur conducted a video surveillance in front of his establishment.
- DSB found that large-scale monitoring of public spaces is in violation of the GDPR

V. New Guidelines / Publications

The European Data Protection Board (EDPB), before Article 29 Working Party, adopted three new guidelines on:

- Certification and identity certification criteria in accordance with Article 42 and 43 of the Regulation 2016/679 and,
- Derogation of Article 49 under Regulation 2016/679
- Territorial Scope of GDPR (Article 3) (public consultation)
- https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

CNIL published its DPIA guidelines, supplementing the G29 Working Party's Opinion

- https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour

The average value of data breach fines issued by ICO doubled over the last year, reaching up to £146.000

- https://dataprotection.news/average-fine-in-uk-for-data-breaches-doubles-to-146000-in-just-a-year/

According to a of the presentation given by the deputy director of the Austrian DSB 100 days after the GDPR became applicable:

- 115 fine proceedings were already pending before the DSB (79 of which were already pending prior to 25 May 2018);
- the DSB had initiated 58 "*ex officio*" investigations;
- 252 data breaches had been notified to the DSB (which seems to be quite on the lower end of the spectrum compared to other jurisdictions); and
- 721 data subject complaints were pending before the DSB at this date

[i] This is a selection made by Niederer Kraft Frey as per 26 November 2018. It shall not represent a complete overview on all recent GDPR Decisions, Lawsuits, Complaints, Fines and Guidelines. This information is not intended to create, and receipt of it does not constitute an attorney-client relationship. You should not rely or act upon this information without seeking professional counsel.

Auftragsbearbeitung – Gesetzliche Grundlagen

- Anwendbarkeit
  - DSG 2
  - DSGVO 3 (2): Bearbeitung von Personendaten von betroffenen Personen in der EU durch einen nicht in der EU niedergelassenen Controller oder Processor, falls im Zusammenhang mit dem Anbieten von Waren/Dienstleistungen an betroffene Personen in der EU oder mit dem Beobachten des Verhaltens betroffener Personen in der EU.
- Anwendbarkeit auf Auftragsbearbeiter
  - DSG: "indirekt"
  - DSGVO: direkt
- Data Controller (DSG 3 i; DSGVO 4 (7) vs. Data Processor (DSG10a; DSGVO 4 (8)
- Wann ist ein Provider ein Auftragsbearbeiter / Data Processor?

  ➔ Definition "Datenbearbeitung"
  - z.B. DSG 3 e. (… "Aufbewahren" …)
  - z.B. DSGVO 4 (2) (… "Speicherung" …)
  - Betrieb eines IT-Systems für den Kunden?
  - Wartung und Support (Applikation, Hardware)?
  - Softwareentwicklung?
- Gesetzliche Haftung
  - DSG: primär Inhaber der Datensammlung/Controller – DSG 34 (DSG 8-10, 14, 6 III, 29)
  - DSGVO: Controller und Processor – DSGVO 79, 82/83
- Umfang / Inhalt Auftragsbearbeitervertrag
  - DSG 10a
  - DSGVO 28

NKF

Checkliste "Auftragsbearbeitervertrag"

- Definitionen
- Hintergrund / Art und Zweck der Bearbeitung (DSGVO 28 (3))
- Umfang (DSGVO 28 (3))
  - Kategorien der durch die Bearbeitung betroffenen Personen und Personendaten: Anhang
- Datenbearbeitung nur auf "dokumentierte Weisung" (DSGVO 28 (3) a
  - Einseitige Weisungen des Auftraggebers?
- Vertraulichkeit (DGSVO 28 (3) b)
  - Besondere Vertraulichkeitsbestimmungen/-erklärungen?
- Sicherheit der Bearbeitung (DSGVO 28 (3) c)
  - Technische und organisatorische Massnahmen (TOMs): Anhang
  - "Akzept" durch Auftraggeber?
  - Standards, z.B. ISO 27001/2
  - DSG 7, 10a II; VDSG 8
- Beizug von Unter-Auftragsbearbeitern (DSGVO 28 (3) d)
  - Generelle Erlaubnis mit "Veto-Vorbehalt"?
  - Einzelgenehmigung von Fall zu Fall?
  - Anhang
- Ausübung der Rechte der betroffenen Personen (DSGVO 28 (3) e)
  - "Unterstützung" des Auftraggebers
  - DSG 8 / VDSG 1
- Weitere Unterstützungspflichten (DSGVO 28 (3) f)
  - Sicherheit (DSGVO 32)

  - Meldung von / Benachrichtigung bei Verletzungen (DSGVO 33, 34)
  - Datenschutz-Folgenabschätzung (UDSGVO 35)
  - Konsultation (DSGVO 36)
- Dauer / Löschung oder Rückgabe (DSGVO 28 (3) g)
- Informationen / Audits (DSGVO 28 (3) h)
  - Lieferung "aller" erforderlichen Informationen zum Nachweis der Einhaltung von DSGVO 28
  - Ermöglichung von / Beitragen zu Audits
  - Kostentragung bei Audits?
  - Standard-Reports?
- Verzeichnis der Verarbeitungstätigkeiten (DSGVO 30)
  - Ausnahmen DSGVO 30 (5) ?
- Garantien bei Datentransfer in "Drittstaaten" (DSGVO 44 ff, insbes. 46) / DSG 6, VDSG 6
- Vertragliche Haftung
  - Eigenständige Regelung?
  - Gemäss Hauptvertrag?
  - DSGVO 82 (2) gesetzliche Haftungsregel

***

27. November 2018

Subject Access Request (SAR) / Anfragen von Datensubjekten

- Rechtliche Bestimmungen
  - Rechtslage gemäss DSGVO
  - Rechtslage gemäss geltendem DSG
- Identifikation
- Zweistufiges Vorgehen (Präzisierung der Anfrage vor Beantwortung)
- Gebrauch von SAR zu anderen Zwecken (Prozessstoff, Beschaffung von Unterlagen)
- SAR-Formular: Gute oder schlechte Idee?
- Erfahrungen mit SAR?

Data Breaches / Meldepflicht

- Rechtliche Bestimmungen
  - Rechtslage gemäss DSGVO
  - Rechtslage gemäss DSG
- Zuständige Datenschutzbehörde
- Meldung an Strafverfolgungsbehörden
- Meldung an Private (Geschäftspartner, Versicherung)
- Erfahrungen mit Data Breaches?

Checkliste SAR (GDPR)

- Erkennen einer Anfrage
- Richtlinie und Prozess, um mündliche SAR zu erkennen
- Verständnis dafür, wann ein SAR abgelehnt werden kann
- Verständnis dafür, welche Informationen herausgegeben werden müssen
- Verständnis dafür, welche zusätzliche Informationen abgeben werden müssen
- Prozess für die rechtzeitige Beantwortung von SAR (inkl. Verlängerung der Frist)
- Verständnis in welcher Form die Antwort erfolgen soll (klare, einfache Sprache)
- Verständnis dafür, wann Personendaten Dritter betroffen sein können

Checkliste Data Breaches (GDPR)

- Erkennen eines Data Breaches
- Vorbereiten eines Data Breach Response Plan
- Verantwortlichkeiten intern verteilen
- Arbeitnehmer schulen
- Arbeitnehmer kennen zuständige Ansprechperson
- Zuständige Behörde kennen
- Wissen, welche Informationen in der Meldung an die Datenschutzbehörde erforderlich sind
- Wissen welche Informationen in der Meldung an die Betroffenen erforderlich sind
- Dokumentation aller Data Breaches, auch den nicht meldepflichtigen

***

27. November 2018

Ihre Ansprechpartner

Clara-Ann Gordon
Partner
clara-ann.gordon@nkf.ch
+41 58 800 84 26

András Gurovits
Partner
andras.gurovits@nkf.ch
+41 58 800 83 77

Voctor Stancescu
Associate
victor.stancescu@nkf.ch
+41 58 800 82 29