Lex Futura
Legal Service Provider

GDPR – One Year Later

Simon Roth

16th May 2019

Lex Futura
Legal Service Provider

Today’s schedule

1. GDPR Enforcement in Numbers
2. Developments in GDPR Case Law and Practice
3. Workshop: GDPR Paint Points in Practice
4. Digest this
5. Apéro and Flying Dinner

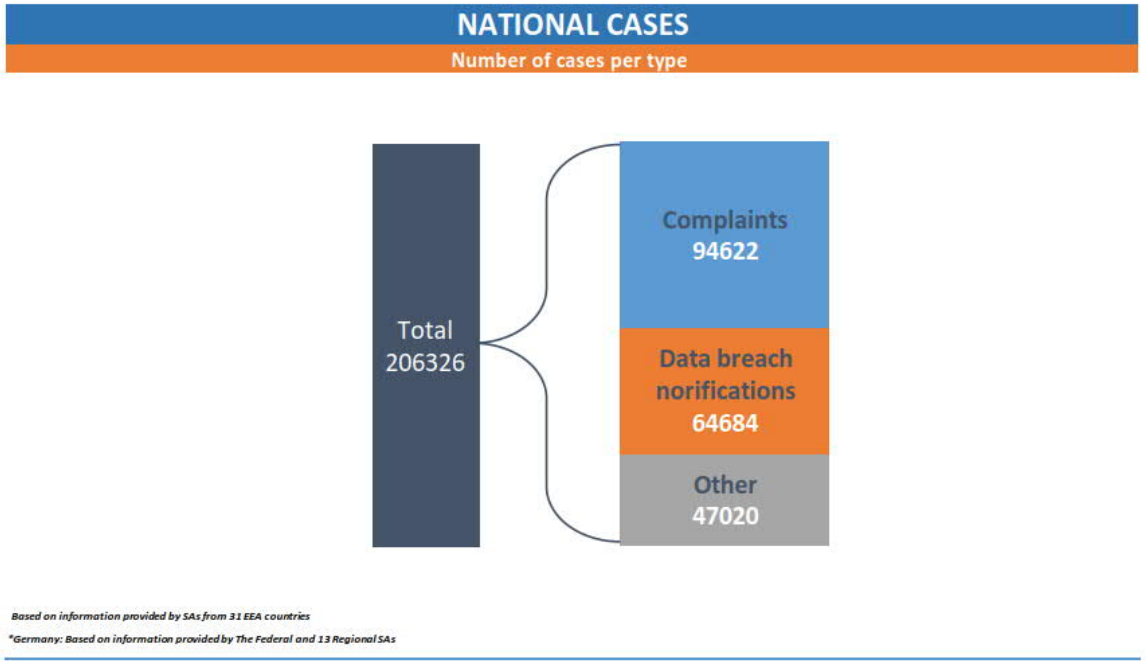
Lex Futura
Legal Service Provider

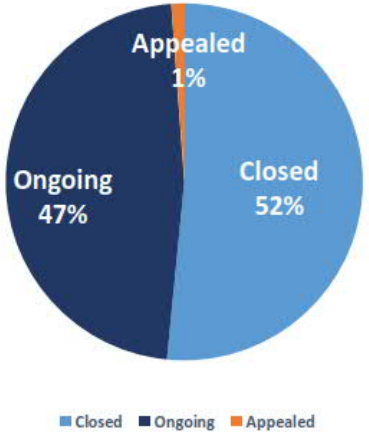
GDPR Enforcement in Numbers

Lex Futura
Legal Service Provider

Cases opened

Implementation and enforcement of the GDPR at national level





Based on information provided by SAs from 31 EEA countries

**Germany: Based on information provided by The Federal and 13 Regional SAs*

Lex Futura
Legal Service Provider

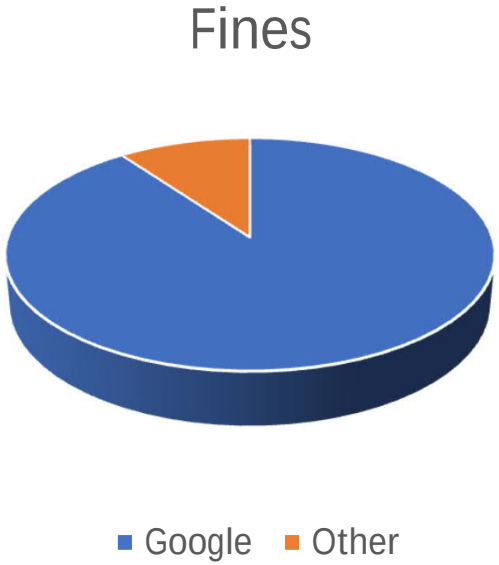
Fines imposed (1/2)

FINES

Number of imposed fines

SAs from 11 EEA countries imposed a total of €55,955,871 fine

Based on information provided by SAs from 11 EEA countries
Germany: Based on information provided by 4 regional SAs

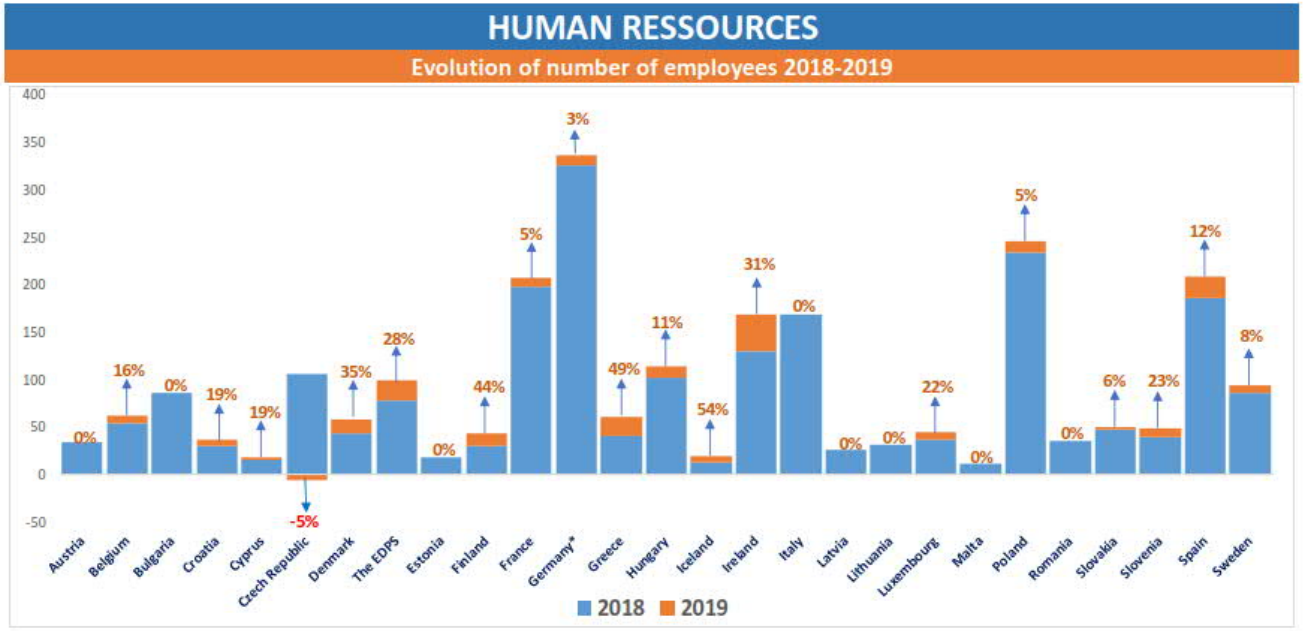


Fines imposed (2/2)

Average fine in Germany = € 6.100,00

Lex Futura
Legal Service Provider

Headcount of regulator

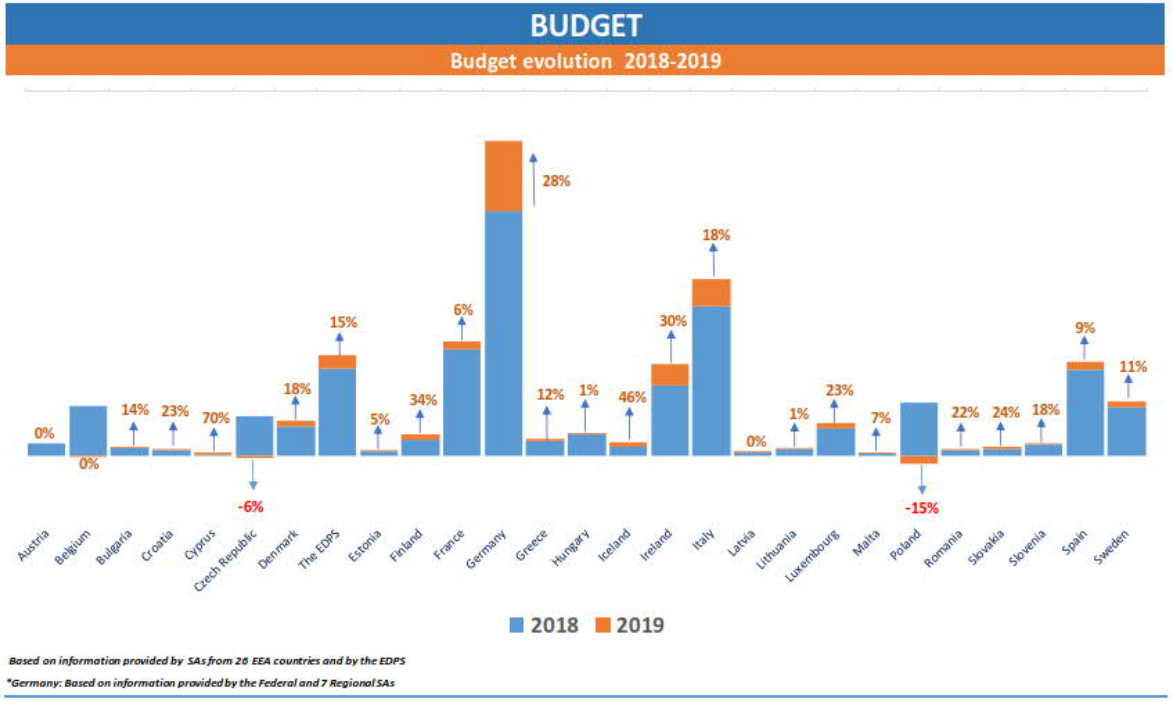


Based on information provided by SAs from 26 EEA countries and the EDPS

** Germany: Based on information provided by 9 Regional SAs*

Lex Futura
Legal Service Provider

Budget of regulator (1/2)

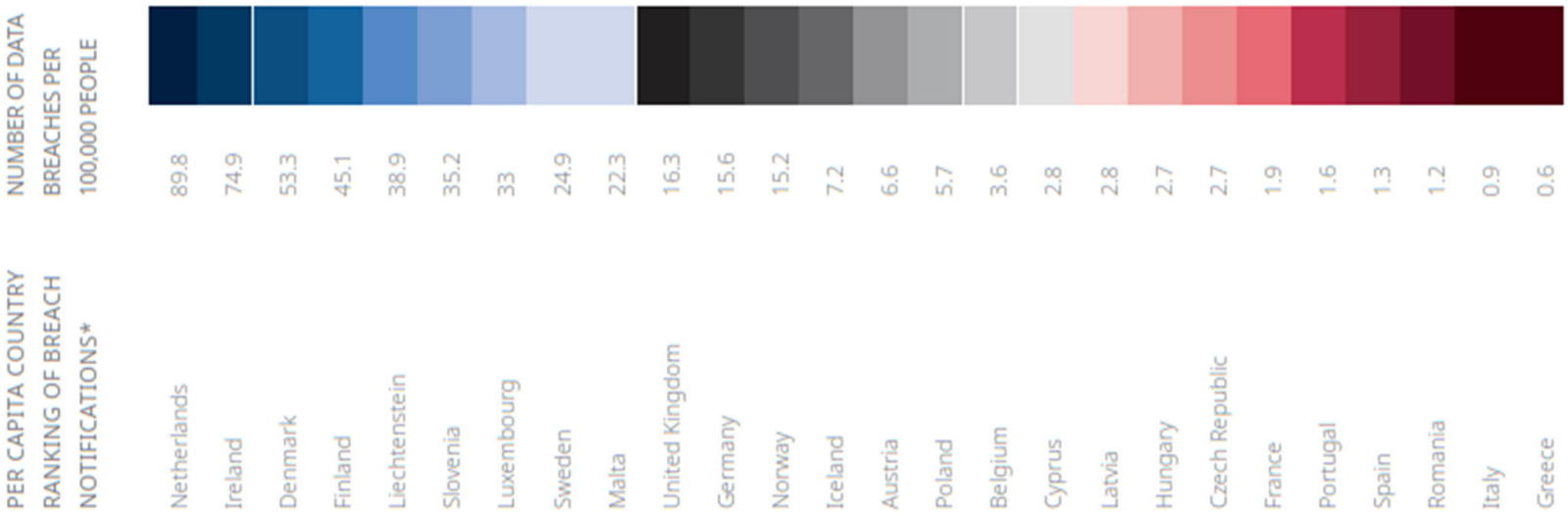


Budget of regulator (2/2)

«Although the majority of the 17 replying Supervisory Authorities stated that they would need an increase in the budget of 30-50%, almost none of them received the requested amount.»

Lex Futura
Legal Service Provider

Data breaches notified



Lex Futura
Legal Service Provider

Developments in GDPR Case Law and Practice

Lex Futura
Legal Service Provider

The GDPR actors

- Court of Justice of the European Union (CJEU)
- Court of Justice of the European Union – Advocate General (AG)
- National Appellate Courts (NAC)
- National Courts (NC)
- European Data Protection Board (EDPB)
- Supervisory Authorities (SA)

Jehova‘s Witnesses (1/3)

CJEU

AG

NAC

NC

EDPB

SA

- Processing personal data in the context of **door-to-door preaching** is not a *«purely personal or household activity»* (which would fall outside of GDPR). — GDPR 2(2)(c)
- **Handwritten notes** taken by door-to-door preachers consisting of names, addresses and religious beliefs constitute a *«filing system»*, which is subject to GDPR although the processing occurs by non-automated means. — GDPR 2(1), 4(6)

Judgment of the CJEU (Grand Chamber) of 10 July 2018, C-25/17, Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta

Jehova‘s Witnesses (2/3)

CJEU

AG

NAC

NC

EDPB

SA

- The community of Jehova’s Witnesses is a joint controller of the personal data processed by the door-to-door preachers even though
  - the community has **no access to the personal data** and
  - the community has **not given written guidelines or instructions** to the preachers in relation to the processing.
- This is because the community *«organizes, coordinates and encourages»* the preaching to *«help to achieve the community’s objective, which is to spread its faith»*.

GDPR
4(7), 26

Judgment of the CJEU (Grand Chamber) of 10 July 2018, C-25/17, Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta

Jehova‘s Witnesses (3/3)

CJEU

AG

NAC

NC

EDPB

SA

(7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes ~~and means~~ of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

GDPR
4(7)

- Focus of the test **lies on purpose**, not on **means**, which has become quite **irrelevant**.
- Taken to the extreme: Appointing someone who furthers your objectives makes you the joint controller of personal data processed by that person in that context.
- In my opinion: **unduly wide definition** of controller but shows were the CJEU was heading to in 2018.

Judgment of the CJEU (Grand Chamber) of 10 July 2018, C-25/17, Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta

Lex Futura
Legal Service Provider

Wirtschaftsakademie (1/4)

CJEU

AG

NAC

NC

EDPB

SA

Judgment of the CJEU (Grand Chamber) of 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig Holstein GmbH

Lex Futura
Legal Service Provider

Wirtschaftsakademie (2/4)

CJEU

AG

NAC

NC

EDPB

SA

- The administrator of a **Facebook fan page** is a **joint controller** of the personal data processed by Facebook.
- This is because:
  - *«the administrator gives Facebook **the opportunity to place cookies** on the computer of a person visiting its fan page»*
  - *«the administrator of the fan page can ask for demographic data relating to its **target audience**, […] and more generally enable it to target best the information it offers.»* (Facebook Insights).

GDPR
4(7), 26

Judgment of the CJEU (Grand Chamber) of 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig Holstein GmbH

Wirtschaftsakademie (3/4)

CJEU

AG

NAC

NC

EDPB

SA

- This is the case notwithstanding that:
  - *«the audience statistics are transmitted to the administrator only in **anonymized** form»*
  - because *«the production of those statistics is based on the **prior collection and the processing** of the personal data of those visitors for such statistical purposes»*
  - and in any event, *«it is **not required** that each of the joint controllers **have access** to the personal data concerned.»*

GDPR
4(7), 26

Judgment of the CJEU (Grand Chamber) of 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig Holstein GmbH

Wirtschaftsakademie (4/4)

CJEU

AG

NAC

NC

EDPB

SA

But:

*«the existence of joint responsibility does **not** necessarily imply **equal responsibility**»*

GDPR
4(7), 26

Judgment of the CJEU (Grand Chamber) of 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig Holstein GmbH

Lex Futura
Legal Service Provider

Joint controller agreements after Wirtschaftsakademie

«Facebook Ireland agrees to take primary responsibility under the GDPR for the processing of Insights Data and to comply with all applicable obligations under GDPR with respect to the processing of Insights Data (including, but not limited to, Articles 12 and 13 GDPR, Articles 15 to 22 GDPR, and Articles 32 to 34 GDPR). Facebook Ireland will also make the essence of this Page Insights Addendum available to data subjects.»

https://www.facebook.com/legal/terms/page_controller_addendum

Lex Futura
Legal Service Provider

Digital marketing after Wirtschaftsakademie

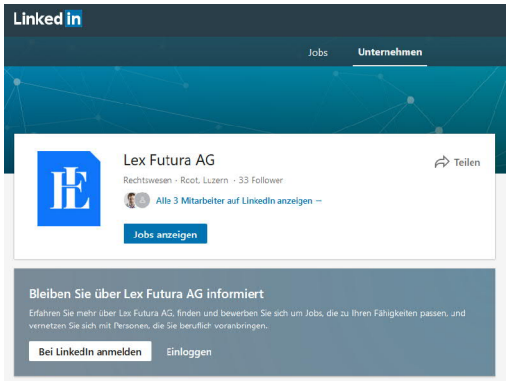
Not a joint controller

Joint controller

To find the location on Google Maps, please follow this link:

https://goo.gl/maps/eh4jcfpW1icUWv6K9

We are looking forward to meeting you.



Lex Futura
Legal Service Provider

Fashion ID (1/4)

CJEU

AG

NAC

NC

EDPB

SA

Advocate General Bobek (born 1977) **highly critical** of *Jehova's Witnesses* and *Wirtschaftsakademie*:

GDPR
4(7), 26

«Will effective protection be enhanced if everyone is made responsible for ensuring it?»

«It is difficult to see how normal users of an online application would not also become joint controllers.»

«Pushed to an extreme, if the only relevant criterion for joint control is to have made the data processing possible, would the internet service provider, or even the electricity provider, then not also be joint controllers potentially jointly liable for the processing of personal data?»

«The intuitive answer is of course 'no'. The problem is that the delineation of responsibility so far does not follow from the broad definition of a controller.»

«A social network, like any other application or program, is a tool. Similar to a knife or a car, it can be used in a number of ways. There is also no doubt that if used for the wrong purposes, that use must be prosecuted. But it might perhaps not be the best idea to punish anyone and everyone who has ever used a knife. One normally prosecutes the person(s) controlling the knife when it caused harm.»

Opinion of Advocate General Bobek of 19 December 2018, C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

Fashion ID (2/4)

CJEU

AG

NAC

NC

EDPB

SA

- AG Bobek proposes to the CJEU to rule as follows:
  - *«A person embedding a third-party plug-in in its website (Like Button), which causes **the collection and transmission of personal data**, is a joint controller together with the service provider (Facebook).»*
  - *«However, that joint responsibility is **limited** to those operations for which **it effectively co-decides on the means and purposes** of the processing of the personal data.»*
  - *«The responsibility **cannot spill over into any potential subsequent stages** of data processing, if such processing occurs outside the control and without the knowledge of the the website operator.»*

GDPR
4(7), 26

Opinion of Advocate General Bobek of 19 December 2018, C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

Lex Futura
Legal Service Provider

Fashion ID (3/4)

CJEU

AG

NAC

NC

EDPB

SA

- If both Facebook and the website operator are joint controllers, **to whom must consent** to data processing (setting of cookies) be given? — GDPR 6(1)(a)
- And **who must give the transparency notice** to the data subject? — GDPR 13, 14
- AG Bobek: to/by the website operator
- However, both consent and notice must **only** cover the **collection and transmission of personal data**, and **not** the subsequent processing by Facebook!

Opinion of Advocate General Bobek of 19 December 2018, C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

Lex Futura
Legal Service Provider

Fashion ID (4/4)

CJEU

AG

NAC

NC

EDPB

SA

- AG Bobek to be lauded for trying to take a more nuanced approach to who should be a (joint) controller and thus potentially liable for GDPR infringements.
- CJEU given the opportunity to put reasonable limits to liability. Will they, however, take AG Bobek's lead?
- Given the breadth of arguments put forward, Fashion ID will be the final precedent on how far liability attaches in digital marketing scenarios.
- The result of Fashion ID will be crucial for assessing the privacy risks of digital marketing in the future.
- Even if the CJEU follows the AG, how to make the distinction between collection and transmission and subsequent processing will need more thoughts to implement in practice.

Opinion of Advocate General Bobek of 19 December 2018, C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.

Planet49 (1/2)

CJEU

AG

NAC

NC

EDPB

SA

- Having to **untick a pre-ticked checkbox** to “not consent” to the data processing (opt-out) is not valid GDPR consent. — GDPR 6(1)(a), 7
- Setting **cookies** requires **consent** by virtue of the **ePrivacy Directive** (ePRD) whether or not — ePRD 5(3)
  - the cookies are **personal data** for the purposes or GDPR, or
  - **other legal bases** (such as legitimate interest) are available under GDPR.
- For consent purposes, the use of a **button** would be preferable over a **checkbox** to make the consent *«separate».* — GDPR 7(2)

Opinion of Advocate General Szpunar of 21 March 2019, C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände e.V.

Planet49 (2/2)

CJEU

AG

NAC

NC

EDPB

SA

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

GDPR 7(4)

- AG Szpunar's **remarkable** statement regarding **the requirement to unbundle consent**:

  *«It should be kept in mind that the underlying purpose in the participation in the lottery is the **'selling'** of personal data. In other words, it is the providing of personal data which constitutes the main obligation of the user in order to participate in the lottery. In such a situation it appears to me that the processing of this personal data is necessary for the participation in the lottery.»*

- If confirmed, controllers could rely on consent in much wider circumstances.

Opinion of Advocate General Szpunar of 21 March 2019, C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände e.V.

Lex Futura
Legal Service Provider

simpli services (Austria)

CJEU

AG

NAC

NC

EDPB

SA

- There is an **absolute rule** against making the performance of a contract conditional on the data subject consenting to the processing of personal data if such processing is not necessary for the performance of the contract.
- No exceptions!
- But obviously wrong if you read GDPR 7(4).

GDPR 7(4)

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Judgment of the Supreme Court of Austria of 31 August 2018, 6 Ob 140/18, Verein für Konsumenteninformation v simpli services GmbH & Co KG.

Lex Futura
Legal Service Provider

AD SPRAY (Italy)

CJEU

AG

NAC

NC

EDPB

SA

- The rule against making the performance of a contract conditional on the data subject consenting to the processing of personal data is **qualified**.
- The authority should enquire whether the services in question can only be obtained through the controller or not. If they can be obtained elsewhere, bundling consent is less problematic.
- At hand, the controller operated a financial news service. Such information can be obtained elsewhere without any difficulty.
- If the user does not want to consent, then he or she should go to the kiosk, and buy a newspaper.

GDPR
7(4)

Judgment of the Supreme Court of Italy of 11 May 2018, 8194/2017, Autorità Garante per la Protezione di Dati Personali v AD SPRAY S.r.l.

Lex Futura
Legal Service Provider

Therapeutic allergens (Germany)

CJEU

AG

NAC

NC

EDPB

SA

- GDPR does not prevent Member States to create a private cause of action in unfair competition if a competitor infringes the GDPR.
- German law makes it an **act of unfair competition** to breach the GDPR.
- A competitor has a right to send a cease and desist letter (***Abmahnung***) to the infringer and then seek an injunction against the infringer.

GDPR
84

Judgment of the Higher Regional Court of Hamburg of 25 October 2018, 3 U 66/17, X v Y

Lex Futura
Legal Service Provider

Whistleblower (Germany)

CJEU

AG

NAC

NC

EDPB

SA

- The right of access is **applicable in the employment** relationship and also while an employment **dispute** is pending in court.
- The employee's access request can be limited where complying with it would adversely affect the rights and freedoms of others.
- However, it is **not sufficient** to generally invoke the **"protection of whistleblowers"** to restrict a former employee's right of access to his HR data.
- The controller that intends to restrict access must **establish the compliance incident** it relies on and show that the rights of the whistleblower outweigh the rights of the employee.

GDPR
15(1), 15(4)

Judgment of the District Labor Court of Baden-Württemberg of 20 December 2018, 17 Sa 11/18, X v Y

Lex Futura
Legal Service Provider

ICANN (Germany)

CJEU

AG

NAC

NC

EDPB

SA

- The collection and publication of **Admin-C and Tech-C** contact information in the **WHOIS** directory **cannot** be based on **consent**. — GDPR 6(1)(a)
- For the simple reason that these persons are not asked for their consent when the registrant registers a URL.
- There is also **no legitimate interest** in collecting and publishing this information. — GDPR 6(1)(f)

Interim Injunction of the District Court of Bonn of 18 July 2018, 10 O 171/18, EPAG Domainservices GmbH v Internet Corporation for Assigned Names and Numbers

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA establishment (1/3)

CJEU

AG

NAC

NC

EDPB

SA

- GDPR applies where the controller has an establishment in the European Economic Area (EEA) **even if** its processing activities are **only directed towards non-EEA** data subjects.

GDPR 3(1)

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA establishment (2/3)

CJEU

AG

NAC

NC

EDPB

SA

- GDPR does not apply to a non-EEA established processor merely because an EEA controller uses the services of this processor.
- However, the controller is **required to use only GDPR-compliant** processors and will ensure this in the **Data Processing Agreement** with the processor.
- Still, the non-EEA processor's liability will be indirect and **contractual only**.

GDPR 3(1)

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA establishment (3/3)

CJEU

AG

NAC

NC

EDPB

SA

- GDPR does not apply to a non-EEA controller merely because this controller uses the services of an EEA processor.
- However, GDPR applies to the EEA processor and it needs to comply with the processor obligations also in relation to the processing for the non-EEA controller.

GDPR 3(1)

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA targeting (1/2)

CJEU

AG

NAC

NC

EDPB

SA

- When considering the targeting criterion, the relevant question is whether such targeting is directed towards data subjects *«who are in the EEA»* at the time of the processing.
- Citizenship, residence or workplace of the data subject is not relevant.

GDPR 3(2)(a)

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA targeting (2/2)

CJEU

AG

NAC

NC

EDPB

SA

GDPR 3(2)(a)

- **Targeting the EEA** must **always** be present under this criterion.
- Merely processing personal data of EEA-located subjects is in itself not sufficient.
- Relevant **elements** for targeting are for example:
  - **Search Engine Optimization** tailored to a EEA country
  - Mentioning **contact points** in the EEA
  - Use of top level domains belonging to EEA countries **(.de, .it, .fr, etc.**)
  - **Testimonials** of EEA customers
  - Payment in **Euro** or other currency only used in an EEA country
  - Using a **language** that is (predominantly) only spoken in a EEA country
  - Offer to deliver ordered goods to an **EEA address**.
- **Not sufficient** in itself: **Accessibility of website** in EEA

Lex Futura
Legal Service Provider

Guidelines on the territorial scope – EEA monitoring

CJEU

AG

NAC

NC

EDPB

SA

- Monitoring must relate to the data subject's **behavior taking place in the EEA**.
- Monitoring includes for example:
  - **Behavioral advertising**
  - Geo-localization
  - Online tracking through cookies and similar technologies
- However, if the controller shows an intention **not to monitor behavior taking place in the EEA**, GDPR does not apply.
- By g**eo-blocking online monitoring** technologies where the visitor accesses from the EEA, you can disapply the GDPR under this criterion!

GDPR 3(2)(b)

Lex Futura
Legal Service Provider

Opinion on the interplay of ePRD and GDPR

CJEU

AG

NAC

NC

EDPB

SA

- The E-Privacy Directive (ePRD) and GDPR **co-exist** (as of today).
- Where ePRD provides for a special rule, **ePRD prevails over GDPR**.
- ePRD therefore prevails over GDPR with regard to the legal basis for **setting cookies**:
  - **Prior consent** from the end user is required, unless the cookie is strictly necessary from a technical point of view.
  - The concept of consent in ePRD is the same as in GDPR.
- However, enforcement of ePRD and sanctions for non-compliance are not governed by GDPR but rather the national law of Member States (which usually provide for much lower fines).

GDPR 95

ePRD 5(3)

Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, adopted on 12 March 2019

Lex Futura
Legal Service Provider

ePrivacy Regulation

- The ePRD is going to be replaced by a **new ePrivacy Regulation** (ePR). However, this change is unlikely to take effect before 2021.
- The latest draft allows to set cookies **without** the end user's **consent** if this is necessary (amongst others)
  - for **audience measuring**,
  - to maintain or restore **security** of an information society service.
- This should at least help around the current problems with Google Analytics, Piwik and other audience measuring tools/cookies.
- But ePR will introduce the same level of fines as for GDPR infringements.

Lex Futura
Legal Service Provider

Endorsement of WP29 guidelines

CJEU

AG

NAC

NC

EDPB

SA

- On 25 May 2018 endorsed previous WP29 guidance with regard to:
  - Lead Supervisory Authority
  - Automated decision-making and profiling
  - Data protection impact assessments
  - Data Protection Officer
  - Rights to data portability
  - Personal data breach notifications
  - Transparency
  - Consent

Lex Futura
Legal Service Provider

CNIL – Fine against Google

CJEU

AG

NAC

NC

EDPB

SA

- On 21 January 2019, the French CNIL fined Google €50,000,000.00 for — GDPR 83
  - **failing** to make the **transparency notice** *«easily accessible»* as the relevant information would have been disseminated over several documents and obtainable only through several steps, and — GDPR 12(1)
  - **failing** to obtain **valid consent for personalized ads** because the consent would not have been *«sufficiently informed»* nor *«specific»* nor *«unambiguous»*. — GDPR 7
- What happened to the **one-stop shop**? — GDPR 60
- Google has appealed the decision.

Decision of the Commission Nationale de l'Informatique et des Libertés of 21 January 2019

Lex Futura
Legal Service Provider

Selection of other fines

CJEU

AG

NAC

NC

EDPB

SA

- Poland, **Bisnode**, €220,000 – data scraping without legal basis.
- Denmark, **Taxa 4X35**, €160,000 – violation of data minimization.
- Portugal, **Hospital near Lisbon**, €400,000 – data breach.
- Germany, **knuddels.de**, €20,000 – data breach.

Lex Futura
Legal Service Provider

Workshop: GDPR Pain Points in Practice

Lex Futura
Legal Service Provider

Some pain points in our experience

Lex Futura
Legal Service Provider

Thank you!