Drinker Biddle

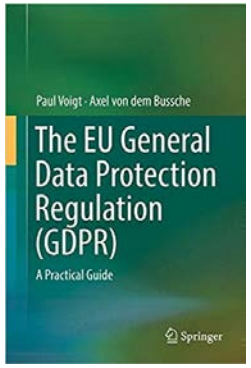
TaylorWessing

GDPR COMPLIANCE COUNTDOWN

April 12, 2018 – T-Minus **43** Days….

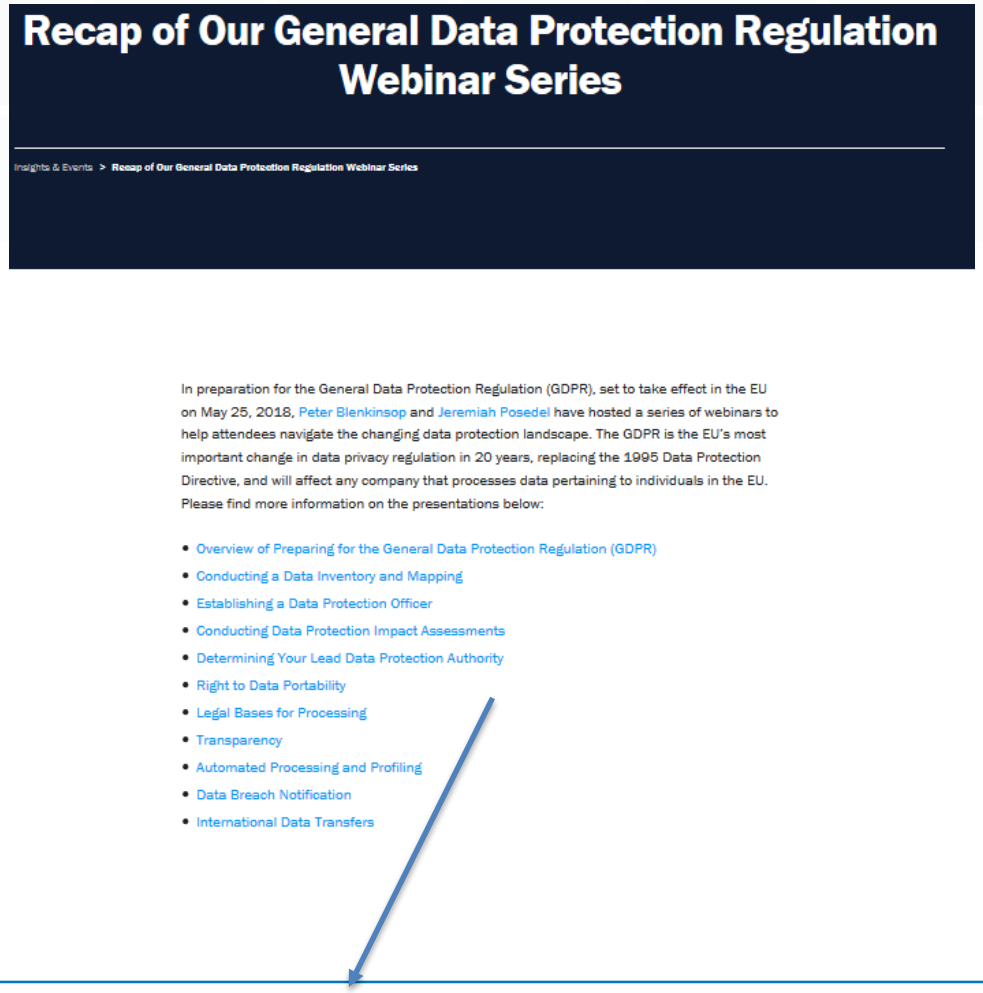
Jeremiah Posedel
Drinker Biddle & Reath
Jeremiah.Posedel@dbr.com
@jposedel

Paul Voigt
Taylor Wessing (Berlin)
P.Voigt@taylorwessing.com



Agenda

- (*Quick*) Overview of GDPR
- Key/Common Issues & Examples
  - *Notice*
  - *Consent*
  - *Legitimate interest*
  - *Facilitating data subject rights*
- Submitted Questions
- Q&A



https://www.drinkerbiddle.com/insights/publications/2018/01/recap-of-our-gdpr-webinar-series

Drinker Biddle

TaylorWessing

(*QUICK*) OVERVIEW OF GDPR

Drinker Biddle

TaylorWessing

(*Quick*) Overview of GDPR

Background

- New EU General Data Protection Regulation (GDPR) published in EU Official Journal on May 4, 2016 and will apply across the EU from **May 25, 2018**.
- Regulation will replace the existing Data Protection Directive and be directly **applicable to all processing of personal data** in the EU / collected from EU data subjects.
- In theory, a goal of the Regulation is to achieve greater harmonization of requirements across EU. However, in many contexts, potential for variation exists.
- Regulation includes significant escalation in potential penalties as compared to current law.
  - Violations can result in fines of up to 4% of an entity's global revenues.

(*Quick*) Overview of GDPR

Territorial Scope

- Applies to processing of "personal data" in the context of the activities of an establishment of a **controller or a processor <u>in the EU</u>**.
- Also applies where a controller or processor is <u>not</u> established in the EU but its processing activities are related to:
  - **Offering of goods or services** to EU residents (regardless of whether payment is provided).
  - **Monitoring** the behavior of EU residents.

(*Quick*) Overview of GDPR

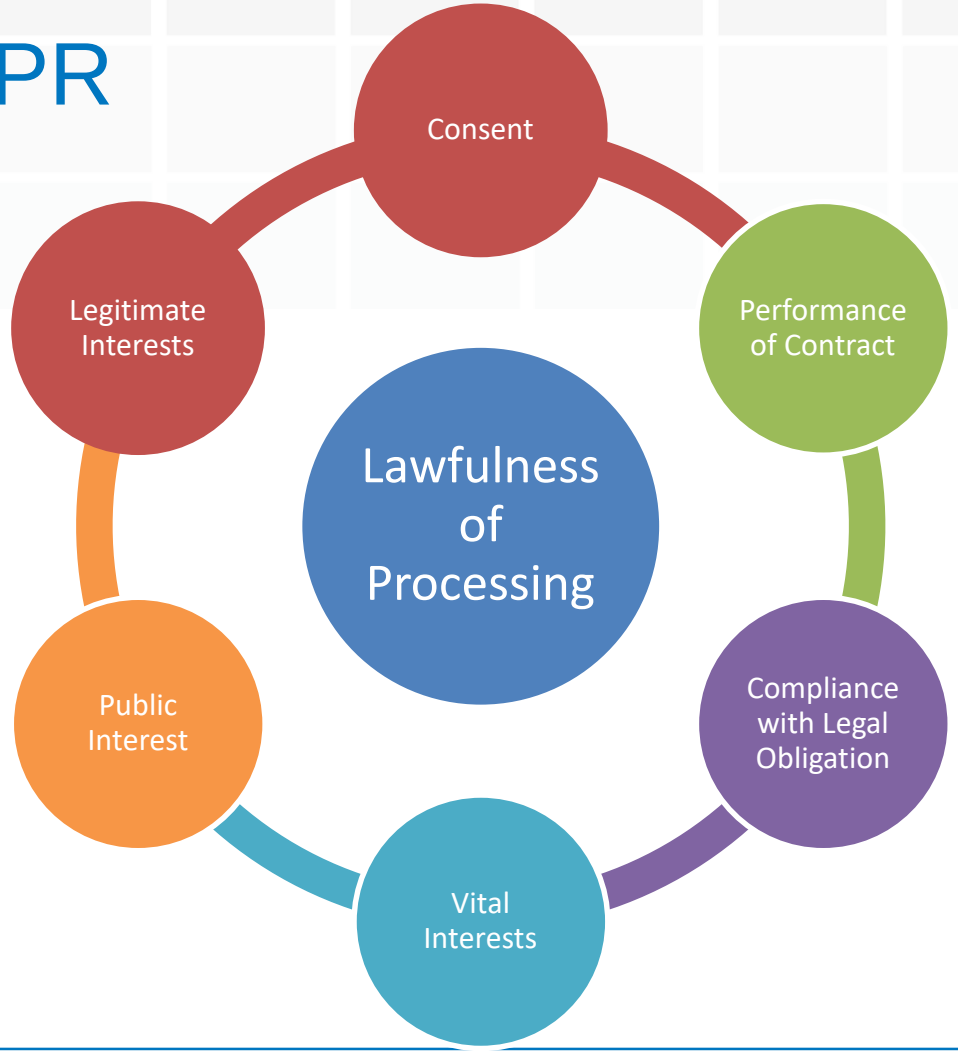
Personal Data

- **Personal data**
  - *Any information relating to an identified or identifiable natural person*.
- **Identifiable person**
  - *Someone who can be directly or indirectly identified, including by reference to a name, an identification number,* ***location data****,* ***online identifier****, or to one or more factors specific to the physical, physiological,* ***genetic****, mental, economic, cultural or social identify of that person*.
  - Pseudonymized data = personal data.

(*Quick*) Overview of GDPR

Legal Bases & Notice

- All processing of personal data requires a **legal basis**.
- Additional requirements when processing **sensitive persona data**.
- Data subjects have the right to receive a data privacy **notice** when data is collected about them.



(*Quick*) Overview of GDPR

Data Subject Rights

- Right of **access** (Art. 15)
- Right to **rectification** (Art. 16)
- Right to **erasure** (Art. 17)
- Right to **restriction** (Art. 18)
- Right to **data portability** (Art. 20)
- Right to **object** (Art. 21)
- Right not to be subject to **decisions based solely on automated processing** which produces legal or similarly significant effects (Art. 22)

(*Quick*) Overview of GDPR

Privacy by Design (PbD) and Data Protection Impact Assessments (DPIAs)

- Data protection must be considered (and such considerations documented) in the design of all new processes and technologies for the processing of personal data.
- Written DPIAs required whenever processing is likely to result in **high risk** to data subjects.
  - Includes (*at least*) processing **sensitive data** and whenever automated **processing/profiling results in decisions having legal effect**.
  - DPIA may evaluate an entire category of processing operations if they are sufficiently similar.
  - DPIA must identify **specific risks** and describe **privacy and security measure**s implemented to mitigate them.
  - Mandatory consultation with data protection authority where processing poses **high level of risk** to data subjects that cannot be adequately mitigated.

(*Quick*) Overview of GDPR

Data Protection Officers

- Companies that process **sensitive data** as core activity or whose core activities involve regular and systematic **monitoring of data subjects** must appoint a data protection officer that reports to the highest levels of management.
- Not required under Directive, but some Member States already require (e.g., Germany).
- Corporate groups may appoint a single, shared DPO.
- DPO must be appointed for fixed term; may be dismissed only for failure to perform duties.
- DPO may perform other duties provided that they do not cause a conflict of interest.

(*Quick*) Overview of GDPR

Records of Processing

- Controllers (and processors) must maintain detailed records on all data processing operations.
- Record-keeping replaces the registration requirements currently in place in some EU countries.
- Controller requirements:
  - Name and contact details
  - Description of processing activity
  - Purpose(s) of the processing
  - Data subject categories
  - Personal data categories
  - Retention period
  - Recipients and third-country transfers
  - Security measures

(*Quick*) Overview of GDPR

Breach Notification

- Data controllers must notify the competent data protection authority without undue delay and, where feasible, **within 72 hours** of becoming aware of a breach, unless it is unlikely to result in a risk to data subjects.
  - Risks include, *inter alia*, physical, material or moral damage to individuals such as discrimination, identity theft or fraud, financial loss, and damage to reputation.
- Data controllers must notify data subjects without undue delay of breaches that are likely to result in a **high risk** to them.
- Breach Categories
  - Confidentiality Breach: Unauthorized or accidental disclosure of, or access to, personal data.
  - Integrity Breach: Unauthorized or accidental alteration of personal data.
  - Availability Breach: Unauthorized or accidental loss of access to, or destruction of, personal data.

(*Quick*) Overview of GDPR

One Stop Shop

- Where processing of personal data spans multiple member states, the **DPA of the entity's European headquarters (or, if different, the DPA of the establishment where decisions concerning the purposes and means of the processing of personal data are taken)**, shall be the lead DPA for oversight and enforcement.
- Nevertheless, each DPA has a defined level of competency to deal with a complaint or possible violation where the subject matter of the complaint/violation concerns only an establishment in the member state of that DPA or substantially affects data subjects only in that member state.
- A cooperation mechanism exists where the lead DPA and other concerned DPAs disagree as to how to handle a case.

Drinker Biddle

TaylorWessing

(*Quick*) Overview of GDPR

International Transfers

- Commission will identify jurisdictions offering adequate data protection.
  - Decisions must be reviewed every four years.
- Appropriate safeguards for transfers to inadequate jurisdictions will include:
  - Binding corporate rules
  - Standard contractual contracts
  - Certification seals for recipient entities
  - Approved industry codes of conduct
- EU-US Privacy Shield still a viable mechanism for transfers to the US.

(*Quick*) Overview of GDPR

Sanctions / Compensation and Judicial Redress

- Violations of a controller's obligations with respect to record-keeping, security, breach notification, and privacy impact assessments are subject to a maximum administrative penalty of €10 million or 2% of the entity's global gross revenue, whichever is higher.
- Violations of a controller's obligations with respect to having a legal justification for processing, complying with the rights of data subjects, and cross-border data transfers are subject to a maximum penalty of €20 million or 4% of the entity's global gross revenue, whichever is higher.
- Data subjects have the right to compensation for any material or immaterial damage resulting from a violation of the Regulation.
- Data subjects can authorize non-profit, public interest bodies to bring complaints on their behalf for the same purposes.
    - Member states are permitted to allow such bodies to independently bring complaints on behalf of data subjects in order to enforce data subject rights and enjoin violations.

Drinker Biddle

TaylorWessing

KEY/COMMON ISSUES & EXAMPLES

Notice

- The controller shall provide the data subject with all of the following information:
  - **identity** and the **contact details** of the controller and, where applicable, of the controller's representative
  - contact details of the **data protection officer**
  - **purposes** of the processing as well as the **legal basis** for the processing
  - where the processing is based on legitimate interest, the **legitimate interests pursued**
  - **recipients** or categories of recipients
  - where applicable, the fact that the controller intends to transfer personal data to a **third country** and the existence or absence of an **adequacy decision**, or in the case of transfers using BCRs, model clauses, codes of conduct, or when transfer is necessary for contract with data subject, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available

Notice (II)

- The controller shall provide the data subject with all of the following information (*continued*):
  - **period** for which the personal data will be stored
  - **existence of the data subject rights** to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
  - where the processing is based on consent, the **existence of the right to withdraw consent** at any time
  - the **right to lodge a complaint** with a supervisory authority
  - whether the provision of personal data is a **statutory or contractual requirement**, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
  - the existence of **automated decision-making**, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
  - ***source*** *the personal data, and if applicable, whether it came from publicly accessible so*urces

Consent

- Consent must be:
  - Freely given
  - Specific
  - Informed
  - Unambiguous indication of individual's wishes
- Individual must be able to withdraw consent at any time without detriment.
- Must maintain a record of consent until related processing is complete.

Consent

Freely Given

- Individual must have a **real choice**, can't feel compelled to consent, and no negative consequences if consent not given.
- Consent **can't be 'bundled'** with acceptance of other terms and conditions.
- Consent **can't be 'tied'** to the provision of a contract or service where the processing is not strictly necessary for the performance of such contract or service.
  - If the controller is able to show that a service includes the possibility to withdraw consent without any negative consequences (e.g., without the performance of the service being downgraded to the detriment of the user), this may show that the consent was given freely.
- **Separate consent** should be possible when engaging in multiple processing activities for more than one purpose.
  - If the controller conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom.

Consent

Freely Given—Examples

- Mobile app allows individuals to log workouts, but asks its users to have their precise GPS location activated for the use of the services. The app also tells its users it will use the collected data for behavioral advertising purposes. Neither geolocalisation or online behavioral advertising are necessary for the provision of the workout collection service and go beyond the delivery of the core service provided.
- When installing Company software, the application asks the user for consent to use non-anonymized crash reports and usage data to improve the software and develop new products and services. Users are informed that they will not be able to use the software unless they consent.

Since users cannot use the app without consenting to these purposes, the consent is invalid (not freely given)

Consent

Specific

- Data subjects must always give consent for a specific processing purpose.
- When seeking consent for various different purposes, there should be a separate **opt-in** for each such purpose ('granularity').
  - Provide specific information with each separate consent request about the data that is processed for each purpose.
  - In the context of direct marketing, consent must be specific to the type of marketing communication in question (e.g., automated call or text message, email, etc.) and the organization sending it.
- If current processing is based on consent and you wish to process the data for a new purpose, must seek a new consent for such new processing purpose.

Consent

Specific—Examples

- Company collects user IMS profile data and usage data, based on user consent, to e-mail them with personal suggestions for new features and applications. After a while, Company decides it would like to also send targeted SMS advertising based on the same user profile data. NEW PURPOSE REQUIRED NEW CONSENT.
- An tradeshow attendee drops his business card into a Company prize bowl at the tradeshow. This is an affirmative act that clearly indicates the individual's agree to his name and contact number being processed for the purposes of the prize draw. HOWEVER, THIS CONSENT WOULD NOT EXTEND TO USING THOSE DETAILS FOR MARKETING OR ANY OTHER PURPOSE.
- An individual submits an online survey about her opinion regarding new functionality deployed in Company software. By submitting the form she is clearly indicating consent to process her data for the purposes of the survey itself. SUBMITTING THE FORM WILL NOT, HOWEVER, BE ENOUGH TO SHOW VALID CONSENT FOR ANY FURTHER USES OF THE INFORMATION.

Consent

Informed

- Minimum information to be provided prior to obtaining consent:
  - Controller's identity.
  - Purpose of each of the processing operations for which consent is sought.
  - Type(s) of data that will be collected and used.
  - The existence of the right to withdraw consent and how to exercise such right.
  - Where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organizations should all be named.
  - E-marketing: Information must cover both the particular organization and the type of communication(s) you want to use (e.g., call, automated call, fax, email, text).

Consent

Informed (II)

- Information must be written using clear and plain language.
  - Long, illegible privacy policies or statements full of legalese not valid.
- Must be clear and distinguishable from other matters.
  - If consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions.
- Easily accessible form.
  - Required information can't be buried in terms of use or privacy policies.
- Must clearly describe the purpose for processing for which consent is requested.

Consent

Unambiguous Indication

- Unambiguous indication of the data subject's wishes.
- Requires a statement or clear affirmative/deliberative act.
  - No pre-ticked boxes / silence or inactivity / merely proceeding with use of service.
- Consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service.
  - Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal.

Consent

Maintaining a Record of Consent

- Obligation of the controller to demonstrate a data subject's consent.
- Should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.
  - In particular, you should record the date of consent, the method of consent, who obtained consent, and exactly what information was provided to the person consenting.
  - Organizations must make sure that they can produce effective audit trails of how and when consent was given in order to give evidence of consent if challenged.

Consent

Withdrawing Consent

- Data subject must be able to withdraw consent at any time without detriment.
- Consent must be capable of being withdrawn by the data subject as easy as giving consent.
  - When consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily.
  - Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface.
- Controller must make withdrawal of consent possible free of charge or without lowering service levels.
- If a customer gives consent when signing up to a service, consent is likely to expire if they subsequently cancel their subscription. The organization should not rely on that consent to send further unsolicited messages to win the customer back.

Legitimate Interest

- Data controller can process personal data where it has a legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests.
  - This interest must be sufficiently articulated and must be real and present.
  - Interests that are "legitimate" may include a broad range of interests, from trivial to compelling, and, at a minimum, must be acceptable under the law.
  - Legitimate interests include "exercise of the right to freedom of expression … conventional direct marketing and other forms of marketing … unsolicited non-commercial messages … enforcement of legal claims … prevention of fraud, misuse of services, or money laundering … employee monitoring for safety or management purposes … whistle-blowing schemes … physical security, IT and network security … processing for historical, scientific or statistical purposes … processing for research purposes."

Legitimate Interest

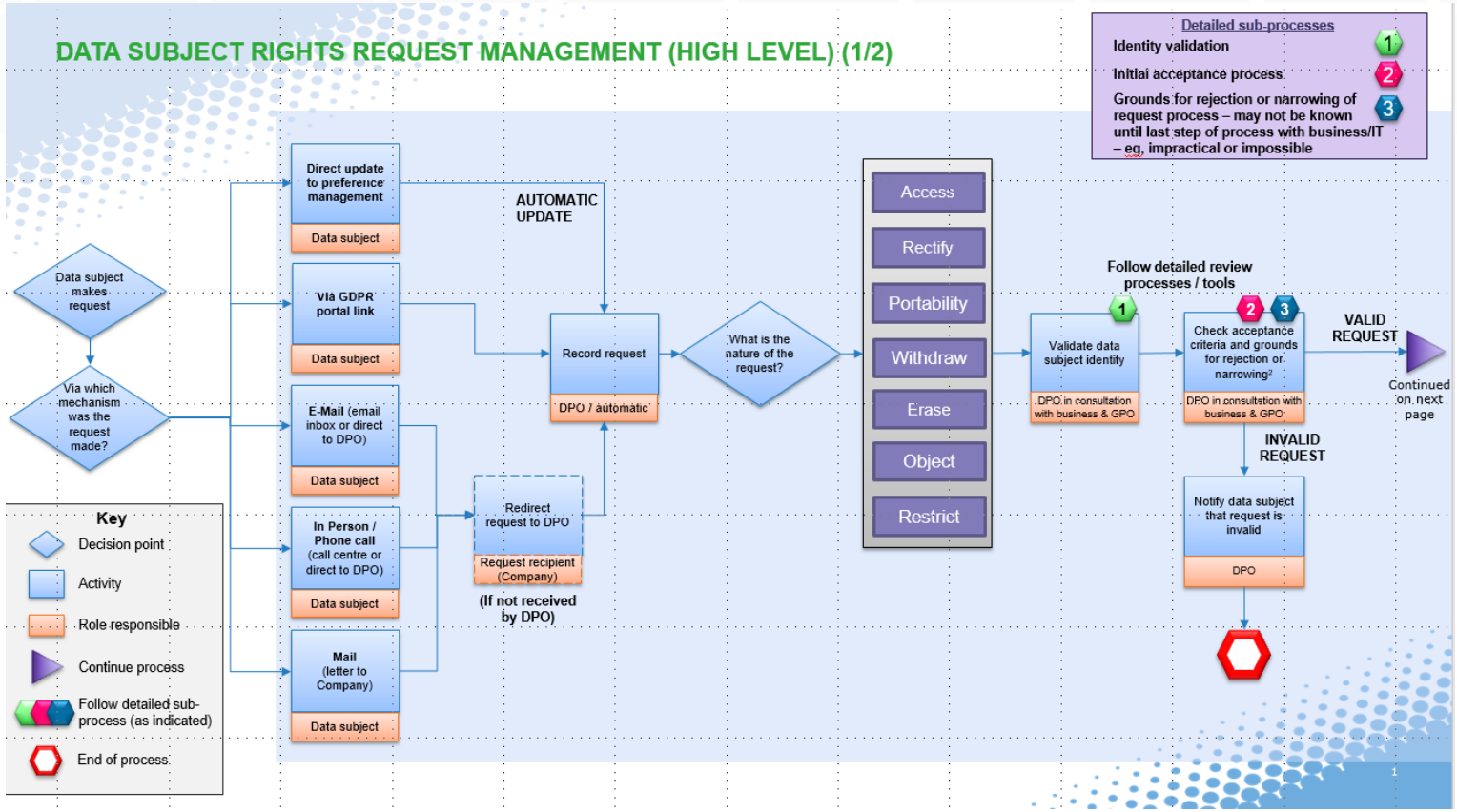
Balancing Test

- Consider the controller's legitimate interest, including:
  - the nature and source of the interest; and
  - any cultural/social recognition of the interest.
- Consider the impact on the data subject, including:
  - the positive or negative consequences of the processing, including psychological impact
  - the nature of the data
  - the way the data is processed
  - the expectations of the data subject
  - the status of the controller in relation to the subject.
- Consider the provisional balance to determine in whose favor the balance tips as a preliminary matter.
- If the provisional balance still leaves doubt, proceed to consider additional safeguards the controller may employ that could limit the undue impact on the data subject (e.g., limitation on data used or immediate deletion after use).

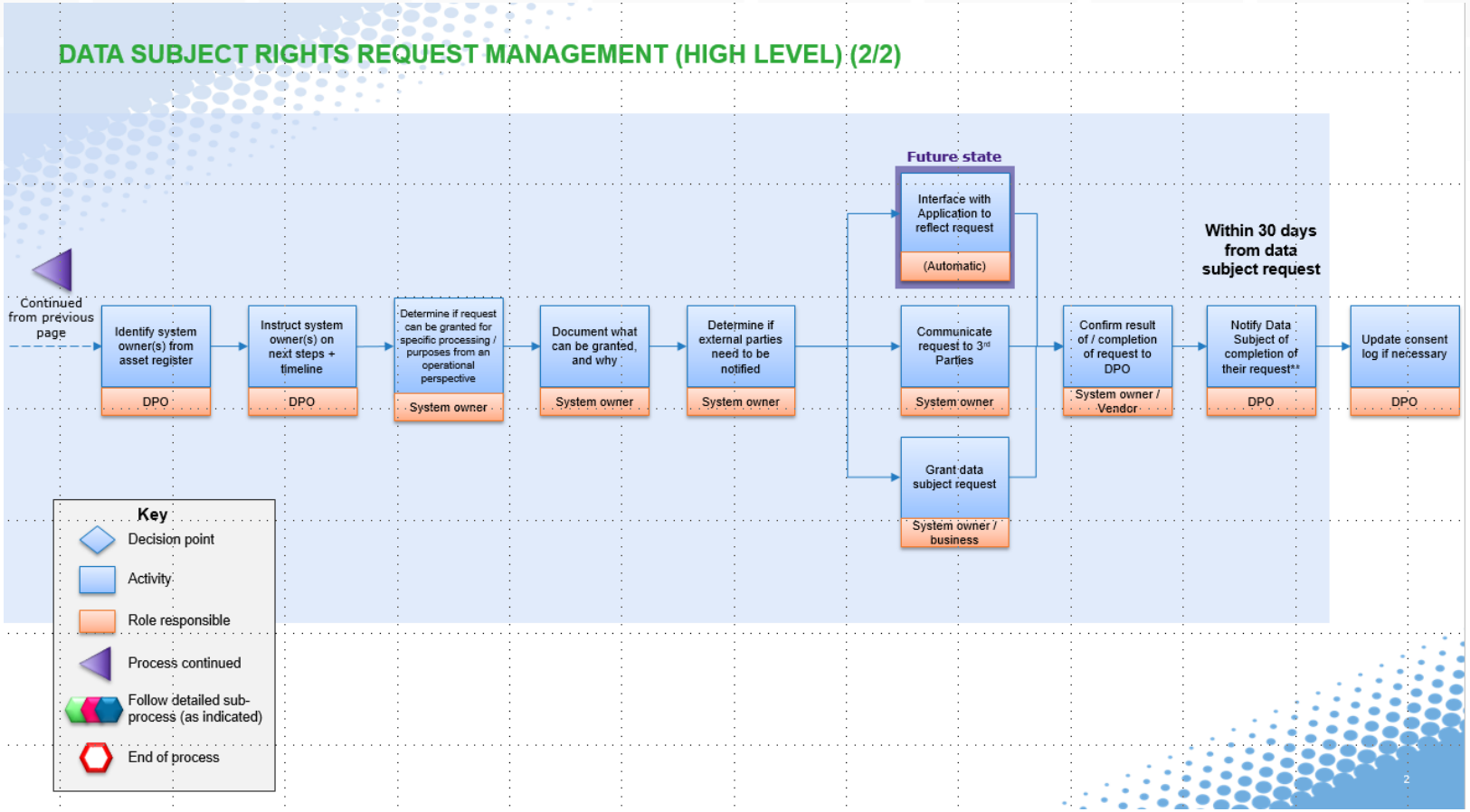
Facilitating Data Subject Rights

- The controller shall facilitate the exercise of data subject rights.
- Form and format of communications
  - Concise, transparent, intelligible and easily accessible form, using clear and plain language.
  - Must be in writing, or by other means, including, where appropriate, by electronic means.
- Response time: without undue delay and in any event within **one month** of receipt of the request.
- Provided free of charge (with some exceptions).
- May request of additional information necessary to confirm the identity of the data subject.
- Notification required even if taking no action on request.

Facilitating Data Subject Rights



Facilitating Data Subject Rights



Drinker Biddle

TaylorWessing

SUBMITTED QUESTIONS

Drinker Biddle

TaylorWessing

Submitted Questions

- Do you expect any tension between the records retention requirements in the U.S. and the data destruction requirements of GDPR?
- How to handle personal data in company mail (Outlook, etc.)?
- If we only have EU data because an EU person enters their info on our website requesting information, what do we need to do?
- Enforcement of GDPR on entities in third countries in the event those entities have no establishment in European Union? How can enforcement be challenged?
- How might GDPR impact a pension fund that provides benefits to retirees and beneficiaries residing in Europe?
- Will controllers still be required to notify/register data transfers (including filing a EU Model Contract) with the DPAs?
- How are companies addressing GDPR notice requirements for marketing contacts?

Drinker Biddle

TaylorWessing

QUESTIONS?