WSGR Getting Ready for the GDPR Series

Overview, main concepts, principles and obligations

Cédric Burton
Of Counsel

Laura De Boel
Senior Associate

Christopher Kuner
Senior Privacy Counsel
Introduction


• Long road: started with the 2010 EU Commission’s communication and ended with the publication of the final text in the EU Official Journal on May 4, 2016.

• Directly applicable in all EU countries.

• One law throughout the EU, but still expect some national deviations:
  – Cultural differences impacting DPAs approaches will most likely remain.
  – Some areas are carved out from the GDPR (e.g., Human Resources).
  – Need to modify local data protection laws.

• Not the end of the road: awaiting future guidance, and significant case law:
  – Court of Justice of the European Union decisions: increased number of data protection-related cases reported lately.
Why should you care about the GDPR?

• Most important piece of EU data protection legislation for next decades.
• Very broad scope of application (both geographical and material).
• Stricter rules and new concepts will have a significant impact on business.
• Obligation to demonstrate compliance with GDPR (accountability principle).
• Increased enforcement and fines (up to 4% of annual worldwide turnover).
• Fully applicable as of May 25, 2018. The clock is ticking!
  – Only 2 years to assess compliance and adapt practices.
  – Changing practice takes time and should be planned in advance.
  – Need to allocate financial and human resources.
Start preparing now! Follow our WSGR Getting ready for the GDPR series

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced individuals’ rights under the GDPR: Notice, right of access, right to be forgotten, data portability, data breach notification.</td>
<td>June 8</td>
</tr>
<tr>
<td>The GDPR for service providers: New obligations, contractual provisions, sub-processing.</td>
<td>July 12</td>
</tr>
<tr>
<td>International data transfers under the GDPR</td>
<td>September</td>
</tr>
<tr>
<td>Regulatory aspects of the GDPR: DPAs’ powers, the EDPB, the one-stop shop, recourse mechanisms.</td>
<td>October</td>
</tr>
<tr>
<td>A panel discussion with leading privacy officers on how to get ready for the GDPR</td>
<td>November</td>
</tr>
</tbody>
</table>
- Verify if the GDPR applies.
- Consider the role of your business.
- Ensure legal ground for data processing.
- Do you process any special categories of data?
- Prepare data processing inventory.
- If required, appoint DPO and carry out PIAs.
- Implement privacy by design and privacy by default.
Does the GDPR apply to your business?

- Companies (controllers and processors) established in the EU:
  - What’s an establishment?
  - Location of data processing is irrelevant.

- Companies (controllers and processors) not established in the EU, but “targeting” EU individuals by:
  - Offering of goods / services to individuals in the EU:
    - Even free of charge.
    - Mere accessibility of website, email address, or contact details is not sufficient as such, but use of EU language or EU currency, or mentioning customers or users in the EU are indicators.
  - Monitoring the behavior of individuals located in the EU:
    - Internet tracking of individuals, in particular, when taking decisions affecting them, or analyzing or predicting their personal preferences, behaviors and attitudes.
Does the GDPR apply to your business?

• If no establishment in the EU, companies must designate a representative in the EU.

• What’s a representative?
  – Natural or legal person explicitly designated in writing.
  – Established in one of the EU countries where individuals whose personal data are processed are located.
  – Represents company re: its obligations stemming from GDPR:
    ▸ Individuals and DPAs can address representative in addition to or instead of the company.
    ▸ DPAs can enforce against representative.
  – Legal actions can be initiated against company, even if representative has been designated (no change of liability).

• Exemption: occasional processing of sensitive data or data relating to criminal convictions or offences, and which is unlikely to result in high risks for individuals.
Material scope

Does the GDPR apply to your business?

- Personal data:
  - Any information relating to an identified or identifiable individual.
  - Any information that can be “linked back” to an individual by anyone and by any means “reasonably likely to be used” (taking into account costs and amount of time required for identification, available technology, and technological developments).
  - Information qualifies as personal data as soon as individual can be singled out.
  - Online identifiers (e.g., IP address, unique device ID, cookie identifiers) and location data are explicitly included in the definition of personal data.
  - Pseudonymized data are data that cannot be attributed to an individual without the use of additional information (e.g., coded data).
    - Pseudonymous data are personal data, but allows for some (limited) flexibility.
    - Pseudonymization is a quasi-mandatory security and “privacy-by-design” measure.

- Anonymized data are not personal data. The GDPR does not apply.
  - But the threshold for anonymization is very high in the EU.
  - De-identified data are unlikely to be anonymous data.
Does the GDPR apply to your business?

• In practice?
  – EU data protection law applies as soon as a company collects or processes personal data of individuals located in the EU.
    ‣ Physical presence or location of data in the EU does not matter.
    ‣ If non-EU controller or non-EU processor, need to appoint a representative in the EU.
  – Concept of personal data is even broader than under the Directive.
    ‣ More difficult to argue that no personal data are processed.
    ‣ All online activities may be captured (e.g., online sale of products, web-based services, online or mobile tracking of individuals located in the EU).
  – Enhanced use of pseudonymization and anonymization techniques.

• How to get ready?
  – Review assessment regarding applicability of EU data protection law.
  – Consider need to appoint representative (who and where).
  – Review company’s processing activities and assess data fields in light of new definitions.
  – Consider option to anonymize or pseudonymize data.
✓ Verify if the GDPR applies.

☐ Consider the role of your business.

☐ Ensure legal ground for data processing.

☐ Do you process any special categories of data?

☐ Prepare data processing inventory.

☐ If required, appoint DPO and carry out PIAs.

☐ Implement privacy by design and privacy by default.
Controller, joint controller and processor (1/2)

• Key concepts for allocation of responsibilities under the GDPR.

• Controller: The entity that, alone or jointly with others, determines the purposes (“why”) and means (“how) of the data processing.
  – Fully responsible for data protection compliance.
  – Joint controllers (“jointly with others”):
    ▶ Joint controllers must have an agreement determining their responsibilities, in particular re: the exercise of individuals’ rights, and controller’s information duties.
    ▶ Essence of the agreement must be available to individuals.
    ▶ Irrespective of the agreement, individuals can turn to any of the joint controllers to exercise their rights.

• Processor: The entity that processes personal data on behalf of and under the instructions of the controller (under data protection agreement / clauses).
  – Under Data Protection Directive, responsible for (minimum): (1) complying with the controller’s instructions (contract); and (2) implementing appropriate security measures.
  – Under the GDPR, many more obligations. Follow our webinar in July!
Controller, joint controller and processor (2/2)

• In practice?
  – Concepts are very similar to those used under the Directive.
  – Need to have mandatory agreements between joint controllers.
  – Transparency requirement regarding the essence of joint controllers’ agreement.
  – Qualification as a processor less advantageous than under the Directive.

• How to get ready?
  – Review your data processing activities and agreements to assess whether your role remains the same.
  – If you are a joint controller, enter into agreement with the other controller(s):
    ▸ Make sure the agreement clearly allocates your respective duties, and its most important terms are available to individuals (e.g., on internet).
  – If you’re a processor, consider whether requalifying as a controller or joint controller would not be more beneficial.
✓ Verify if the GDPR applies.

✓ Consider the role of your business.

☐ Ensure legal ground for data processing.

☐ Do you process any special categories of data?

☐ Prepare data processing inventory.

☐ If required, appoint DPO and carry out PIAs.

☐ Implement privacy by design and privacy by default.
Legal grounds for processing (1/4)

• GDPR maintains the existing legal grounds for data processing but restricts them.
• Main legal grounds from business perspective are:
  – Consent;
  – Performance of contract; and
  – Legitimate interests of controller or third party.
• GDPR introduces VERY strict conditions for consent to be valid.

<table>
<thead>
<tr>
<th>Conditions for consent</th>
<th>What does this mean?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear, affirmative and unambiguous</td>
<td>Individual gives consent by clear and affirmative action.</td>
</tr>
<tr>
<td></td>
<td>Silence, pre-ticked boxes or inactivity does not mean consent.</td>
</tr>
<tr>
<td>Informed</td>
<td>Individual must be aware at least of: (1) controller’s identity; (2) purposes of processing; and (3) possibility to withdraw consent.</td>
</tr>
<tr>
<td>Specific</td>
<td>No consent “hidden” in Privacy Policy or T&amp;Cs.</td>
</tr>
<tr>
<td></td>
<td>One consent covers all processing activities for the same purpose.</td>
</tr>
<tr>
<td></td>
<td>If more purposes, consent must be given for each of them.</td>
</tr>
<tr>
<td></td>
<td>Prohibition of “bundled” consent.</td>
</tr>
</tbody>
</table>
Legal grounds for processing (2/4)

<table>
<thead>
<tr>
<th>Conditions for consent</th>
<th>What does this mean?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freely given</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• It must be genuine and free choice, and individuals must be able to refuse or withdraw it at any time without detriment.</td>
</tr>
<tr>
<td></td>
<td>• Not valid when clear imbalance between individual and controller.</td>
</tr>
<tr>
<td></td>
<td>• Presumption that consent is not freely given when:</td>
</tr>
<tr>
<td></td>
<td>• Individual is not allowed to give separate consent to different processing activities.</td>
</tr>
<tr>
<td></td>
<td>• Provision of service depends on consent while it is not necessary for the performance.</td>
</tr>
</tbody>
</table>

• Request for consent:
  – Presented clearly, in intelligible and easily accessible form, in clear and plain language.
  – Should not contain unfair terms.
  – Must be distinguishable from other part of the document which deals with other matters.
  – If electronic, it must be concise and not unnecessarily disruptive.

• Possibility to obtain electronic consent by (1) ticking a box online; or (2) selecting technical settings for internet-based services.

• Burden of proof is on the controller!
• Balancing of interests:
  – Interests of controller or third party vs. data protection rights of individuals.

• GDPR restricts applicability of this legal basis:
  – Interests of controller must meet reasonable expectations of individuals, based on their relationship with controller.
  – Companies must inform individuals of legitimate interests basis in privacy notice.
  – Individuals have the right to object at any time to the processing.
  – Document rationale for relying on legitimate interest.
  – Burden of proof is on the controller.

• Processing strictly necessary for the following purposes constitutes legitimate interests:
  – Fraud prevention.
  – Ensuring security of network and information systems, and security of related services offered through such networks and systems.

• Depending on the context, the following may constitute legitimate interests of controller:
  – Relevant and appropriate client – controller relationship.
  – Internal administrative purposes within group of companies.
Legal grounds for processing (4/4)

• In practice?
  – Higher threshold for legal grounds to be valid.
  – Burden of proof is on the controller.
  – If there’s doubt whether consent is freely given (e.g., because of potential imbalance between individual and your company), assess whether you can rely on other legal basis.
  – Such other legal basis could be the legitimate interests of the controller or a third party.
  – Need to document how consent is obtained and the assessment of the legitimate interests.
  – Legitimate interests must be specifically mentioned in privacy notice.

• How to get ready?
  – Assess legal bases for all data processing activities (by purpose) of your company.
  – Document the rationale for relying on one legal ground over another.
  – Gather existing consent languages and forms.
  – Assess whether all existing consent practices and forms comply with stricter rules.
  – Assess whether your interests prevail individuals’ interests:
    ▸ Can individuals reasonably expect at the time of data collection that processing for this purpose may take place?
    ▸ Provide possibility to opt-out to the processing to which individuals can object.
✓ Verify *if* GDPR applies.

✓ Consider the role of your business.

✓ Ensure legal ground for data processing.

☐ **Do you process any special categories of data?**

☐ Prepare data processing inventory.

☐ If required, appoint DPO and carry out PIAs.

☐ Implement privacy by design and privacy by default.
Special categories of data (1/3)

• Broader definition of **sensitive data**:
  – GDPR adds new type of data: data concerning an individual’s sexual orientation, genetic data, and biometric data processed to uniquely identify an individual.

• New definitions:
  – **Data concerning health**: personal data related to the physical or mental health of an individual, including the provision of health care services revealing health status.
  – **Biometric data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual, which allow his or her unique identification (e.g., facial images or dactyloscopic data).
  – **Genetic data**: personal data relating to the inherited or acquired genetic characteristics of an individual which give unique information about his or her physiology or health, and which result, (e.g., from analyzing biological sample).

• Limited legal grounds, such as explicit consent, and stricter application of GDPR (PIA, DPO).

• Member States can impose conditions on processing of health, biometric and genetic data.
• Processing children’s data requires parental consent.

• Who’s a child under GDPR? Individuals below sixteen, except if EU Member States law lowers the threshold (with a minimum of thirteen).

• Applies when children’s data are processed in the context of ‘information society services’ (i.e., services normally provided for remuneration, at a distance, by electronic means and at the individual request).

• Controllers must make “reasonable efforts” to verify parental consent, taking into consideration available technology.

• Many questions remain open due to lack of guidance:
  — Does the parental consent requirement apply only to child-specific services or to all services?
  — What do “reasonable efforts” to verify parental consent mean? Obligation to verify age of children?
  — When companies are not in position to verify parental consent due to the limits of “available technology”?
  — Conditions for valid parental consent?
Special categories of data (3/3)

• In practice?
  – Concept of sensitive data is broadened.
  – More data processing activities will require individual’s explicit consent.
  – Stricter obligations apply. Significant impact on some sectors.
  – Companies offering internet-based services to children will have to implement verification processes for (i) children’s age, and (ii) parental consent.

• How to get ready?
  – Review all data fields to assess whether they fall under any of the new definitions.
  – Review the legal bases on which you collect sensitive data.
  – Assess whether you offer internet-based services to individuals whose age is less than 16.
  – Survey EU countries to identify where age limit is different.
  – Consider how your company can verify child’s age and obtain valid parental consent.
  – Establish processes to document how parental consent is obtained.
✓ Verify if the GDPR applies.
✓ Consider the role of your business.
✓ Ensure legal ground for data processing.
✓ Do you process any special categories of data?

☐ Prepare data processing inventory.

☐ If required, appoint DPO and carry out PIAs.

☐ Implement privacy by design and privacy by default.
Internal records (1/2)

• GDPR repeals the obligation to file registration with national DPAs.
• Instead, GDPR requires companies (controllers and processors) to keep internal records of data processing activities (i.e., data inventories) that must be communicated to DPA upon request.
• Companies employing fewer than 250 employees are exempt from this requirement unless their data processing activities:
  – Are likely to result in risks to individuals;
  – Are repetitive; or
  – Include sensitive data or data relating to criminal convictions and offences.
• Prescriptive content of internal records for controllers:
  – Name and contact details of the controller, joint controller, representative and Data Protection Officer (DPO);
  – Purposes and categories of (i) individuals, (ii) personal data and (iii) data recipients;
  – Information re: data transfers and documentation of safeguards;
  – Information re: data retention (if possible) and description of security measures.
• Expect some guidance on this topic.
Internal records (2/2)

• In practice?
  – Shift from filing registrations with DPAs to keeping internal records of processing activities.
  – Red tape reduced? Gathering information about all processing activities, documenting and keeping them up-to-date will involve company’s resources.
  – No guidance on how to count company’s employees.

• How to get ready?
  – Assess whether your company is exempt from the internal records requirement.
  – If not:
    ▶ Gather information on your processing activities and begin documenting them.
    ▶ Create template data inventory.
    ▶ Implement internal processes to ensure that your records are up-to-date.
    ▶ Train your staff so that it is aware of the records and of the process to update them.
✓ Verify if GDPR applies.

✓ Consider the role of your business.

✓ Ensure legal ground for data processing.

✓ Do you process any special categories of data?

✓ Prepare data processing inventory.

☐ If required, appoint DPO and carry out PIAs.

☐ Implement privacy by design and privacy by default.
Data Protection Officer (1/2)

• General rule: companies (controllers and processors) may appoint a DPO.
• Mandatory appointment of a DPO:
  – Large-scale, regular and systematic monitoring of individuals.
  – Processing of sensitive data and data relating to criminal convictions and offences (must be the company’s core data processing activities).
  – National laws (e.g., Germany) may require companies to appoint a DPO in other cases.
• A group of companies may appoint a single DPO if easily accessible from each establishment.
• Main tasks of DPO:
  – Advises company and its staff on GDPR obligations.
  – Monitors compliance with GDPR and internal privacy policies (e.g., assignment of responsibilities; awareness-raising; trainings; audits).
  – Provides advice on PIA and monitors its performance.
  – Cooperates with DPA and acts as its contact point (e.g., in case of DPA consultation).
• DPO qualifications:
  – Expert knowledge in data protection law and practices.
  – Ability to fulfill his / her tasks.

Wilson Sonsini Goodrich & Rosati, LLP
Data Protection Officer (2/2)

• Companies’ obligations:
  – Publish the DPO contact details and notify them to DPA.
  – Involve DPO in all data protection issues.
  – Provide DPO with resources necessary to: (1) perform his or her tasks; (2) access personal data and data processing activities; and (3) maintain his or her expert knowledge.

• Position of DPO:
  – May be a member of staff or a contractor, but should be able to perform tasks independently.
  – Can fulfil other tasks as long as there is no conflict of interest.
  – Cannot receive instructions, and cannot be dismissed or penalized for performing tasks.
  – Must directly report to the company’s highest management level.
  – Is bound by confidentiality / secrecy obligation.

• Individuals may contact DPO on any matter re: processing of their personal data.

• Expect guidance on designating DPO!
• Mandatory PIA in three specific cases:
  – Systematic and extensive evaluation of individuals’ personal aspects, based on automated processing, and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect them.
  – Large-scale processing of sensitive data or of personal data relating to criminal convictions and offences.
  – Large-scale and systematic monitoring of public area.
• For other processing activities, PIA is required if they are likely to result in high risks.
• In addition, DPA can consider that a PIA is required because, e.g.:
  – Individuals are prevented from exercising their rights or using service or contract.
  – Processing activities are carried out systematically on a large scale.
• Exemptions: PIA is not mandatory if processing concerns personal data from patients or clients of: (1) individual physician; (2) other health care professional; or (3) lawyer.
• If appointed, DPO must be consulted.
Privacy Impact Assessment (2/2)

- Minimum content of PIA is specified in the GDPR.
- If outcome of PIA = high risks:
  - Obligation to implement mitigating measures (demonstrating compliance with GDPR).
  - If not possible to mitigate high risk (e.g., because of available technology or costs of implementation), companies must consult DPA prior to the processing.
- Expect guidance on notion of high risks and PIA before GDPR is enforceable.
- More regulatory guidance later on:
  - DPAs will publish list of processing activities requiring PIA.
  - DPAs may publish list of processing activities not requiring PIA.
  - EDPB may indicate processing activities for which a PIA is not necessary, and indicate sufficient measures to conduct such activities.
Data Protection Officer and Privacy Impact Assessment

• In practice?
  – DPO will become a key element of an EU data protection compliance program.
  – Strict requirement of DPO independence.
  – For many processing activities, PIAs will be required or strongly recommended.
  – DPO will be ultimately responsible for PIAs.

• How to get ready?
  – Assess whether your company is required to appoint a DPO: check national laws.
  – Even if not required, consider appointing a DPO.
  – If you appoint a DPO: (1) reserve necessary resources; and (2) ensure DPO’s independency.
  – Develop template PIAs.
  – Document PIAs to demonstrate compliance with GDPR.
  – Look for guidance on notion of high risk and PIA once it’s published.
✓ Verify *if* GDPR applies.

✓ Consider the role of your business.

✓ Ensure legal ground for data processing.

✓ Do you process any special categories of data?

✓ Prepare data processing inventory.

✓ If required, appoint DPO and carry out PIAs.

☐ **Implement privacy by design and privacy by default.**
Privacy by design and privacy by default

- GDPR introduces obligation to build privacy in products and services early at the stage of conception and during the entire product/service lifecycle.

- **In practice?**
  - Privacy by design: embedding privacy in new technologies, products and services:
    - For companies: data minimization, pseudonymization or encryption.
    - For individuals: allowing them to exercise their rights.
    - For processors: enabling controllers to comply with the GDPR.
  - Privacy by default: the most protective approach should be the default.

- **How to get ready?**
  - Assess how internal processes can be adjusted.
  - Create internal policies and procedures to ensure that privacy is taken into account at the earliest stage of product development.
  - Raise privacy awareness via training.
  - Document privacy considerations in entire product lifecycle.
Conclusions

- GDPR is built on the same core principles as the Directive, but it introduces many changes and much stricter rules!
- The GDPR is a game-changer; enforcement risk will be much higher.
- Use the 2-year transition period wisely.
- Changing practices takes time and should be planned in advance.
- Follow WSGR webcast on the GDPR overview. Stay tuned for our next webcasts!

<table>
<thead>
<tr>
<th>Enhanced individuals’ rights under the GDPR: Notice, right of access, right to be forgotten, data portability, data breach notification</th>
<th>June 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>The GDPR for service providers: New obligations, contractual provisions, sub-processing</td>
<td>July 12</td>
</tr>
<tr>
<td>International data transfers under the GDPR</td>
<td>September</td>
</tr>
<tr>
<td>Regulatory aspects of the GDPR: DPAs’ powers, the EDPB, the one-stop shop, recourse mechanisms</td>
<td>October</td>
</tr>
<tr>
<td>A panel discussion with leading privacy officers on how to get ready for the GDPR</td>
<td>November</td>
</tr>
</tbody>
</table>
Questions?

Thanks!

Cédric Burton
Of Counsel
cburton@wsgr.com

Laura De Boel
Senior Associate
ldeboel@wsgr.com

Christopher Kuner
Senior Privacy Counsel
ckuner@wsgr.com

WSGR Regulation Observatory:
www.wsgr.com/EUDataRegulation
WSGR resources

• WSGR EU Data Protection Observatory (with full background information and analysis of the GDPR, legislative texts, and all articles cited below): www.wsgr.com/EUDataRegulation.

• WSGR Data Advisor: www.wsgrdataadvisor.com.


