WSGR Getting Ready for the GDPR Series

Session 2: Enhanced Individuals' Rights

Cédric Burton
Of Counsel

Laura De Boel
Senior Associate

Wilson Sonsini Goodrich & Rosati, LLP

WSGR Webinar, Brussels, June 8, 2016

Introduction

- EU data protection law grants individuals rights to their personal data.
- The rationale is to empower individuals.
- One of the most significant topic under EU data protection law.
- As of May 25, 2018, the EU General Data Protection Regulation (GDPR) will be fully effective.
- The GDPR enhances individuals' rights.
- Responsibility for allowing individuals to exercise these rights lies with the controller.
- Role for processors to enable controllers to be compliant with GDPR.
- Controllers will risk fines of up to 4% of annual worldwide turnover if they don't allow individuals to exercise their rights.
- To help companies prepare for GDPR, WP29 and DPAs will issue guidance.

Start preparing now! Follow our WSGR Getting ready for the GDPR series

The GDPR for service providers: New obligations, contractual provisions, sub-processing.	**July 12**
International data transfers under the GDPR.	September
Regulatory aspects of the GDPR: DPAs' powers, the EDPB, the one-stop shop, recourse mechanisms.	October
A panel discussion with leading privacy officers on how to get ready for the GDPR.	November

Enhanced Individuals' Rights

GDPR enhances existing rights:

1. Notice right (transparency requirements).
2. Right of access.
3. Right to rectification.
4. Right to restriction.
5. Right to object.
6. Right to erasure ("right to be forgotten").
7. Right not to be subject to automated decision making.

…and introduces new rights:

1. Right to data portability.
2. Data breach notification requirements.

Notice to Individuals (1/4)

- Privacy notice and any communication with individuals should be:
  - concise;
  - transparent;
  - intelligible;
  - easily accessible; and
  - the language should be clear and plain, especially when addressed to a child.
- GDPR significantly increases the amount of information that controller must provide to individuals:

Information in Privacy Notice	Directive	GDPR
Identity and contact details of the controller and its representative (if any)	✓	✓
Identity and contact details of DPO	N/A	✓
Purposes of the processing	✓	✓
Legal basis for the processing, including legitimate interests	N/A	✓
Data recipients	✓	✓
Categories of personal data (if data were not obtained from the individual)	✓	✓
Intention to transfer data outside the EU and information about: • existence or absence of adequacy decision; • legal basis for data transfers; • reference to suitable safeguards; and • means to obtain a copy of safeguards (e.g., model contract) / where they are available (e.g., a hyperlink).	N/A	✓

Notice to Individuals (2/4)

- Additional information as necessary to ensure fair and transparent processing:

Information in Privacy Notice	Directive	GDPR
Data retention period / criteria used to determine this period	N/A	✓
Existence of right of access and rectification	✓	✓
Existence of other individuals' rights (i.e., right to erasure, restriction, objection, data portability).	N/A	✓
Right to withdraw consent at any time, without affecting lawfulness of data processing prior to withdrawal	N/A	✓
Right to lodge a complaint with DPA	N/A	✓
Whether providing data is a statutory or contractual requirement, or necessary to enter into a contract	N/A	✓
Whether replies to questions are mandatory, and consequences of failure to reply	✓	✓
Source of the personal data (if data were not obtained from the individual). When the origin of the data cannot be provided because various sources have been used, general information should be provided.	N/A	✓
Existence of automated decision making, and at least meaningful information about: - logic involved and significance and - consequences of such processing for the individual.	N/A	✓

Notice to Individuals (3/4)

- Timing:
  - When data are obtained.
  - Where data are not obtained directly from individuals:
    - Within “reasonable period,” but at the latest within one month after obtaining the data.
    - At the latest at the time of the first communication with the individual, if data are used to communicate with individual.
    - At the latest when data are first disclosed to another data recipient.
- Exemptions:
  - If individual already has the information. Burden of proof lies with the controller!
  - If data are not obtained directly from individuals, and:
    - Impossible to provide information; disproportionate effort; or the disclosure would render impossible or seriously impair the achievement of the objectives of the processing (e.g., scientific or statistical purposes).
    - Obtaining such data is based on EU or Member State law.
    - Data must remain confidential due to professional secrecy obligations imposed by EU or Member State law.
- Option to use standardized icons (not mandatory):
  - Not yet available; EU Commission will specify the standardized icons and the way to provide them.
  - The goal is to give an overview of processing in an easily visible and intelligible way.
  - If presented electronically, icons should be machine-readable.

Notice to Individuals (4/4)

- **In Practice?**
  - Comprehensive and lengthy privacy notices.
  - Include information regarding how individuals can exercise their rights.
  - Need to keep privacy notices updated.
- **How to Get Ready?**
  - Gather all privacy notices and policies.
  - Prepare template language.
  - Consider providing layered privacy notices, especially for small screen devices.
  - In case you're exempt from providing notice, be ready to prove it.
  - Update your privacy notices.
  - Publish your privacy policy online if data are not collected directly from individuals and providing specific notice proves to be impossible.
  - Train your staff about the notice requirement. Two key points to remember:
    - Provide notice at the time of data collection; and
    - Adapt notice to the processing in question.
  - Monitor DPAs guidance on privacy notices and EU Commission guidance on standardized icons.

Right of Access (1/3)

- GDPR strengthens it and makes it more comprehensive.
- Essence: right to obtain confirmation as to whether data is processed, to obtain a copy of the data, and information regarding the data processing.
  - Individuals may exercise this right at reasonable intervals.
  - The goal is for individuals to be aware of processing and to verify its lawfulness.
- Right to obtain a copy:
  - Controller can verify the identity of the individual through all reasonable means (e.g., copy of ID card).
  - Exceptions:
    - Not an absolute right: it should not adversely affect rights and freedoms of others.
    - If requests are "manifestly unfounded or excessive, in particular because of their repetitive character," the controller may charge a reasonable fee or refuse to act on the request. Burden of proof lies with the controller!
    - A refusal to comply with the request must be reasoned, and individuals should be informed of the possibility to lodge a complaint with DPA and seek judicial remedy.
  - Initial copy must be free of charge, but controllers may charge a reasonable fee for further copies.
  - If the request is made by electronic means: obligation to use a "commonly used electronic form."
- Timing: without undue delay, but max. within one month of the request.
  - Possibility to extend to two months if complex and large number of requests.
  - Controller has one month to inform the individual of the extension and reasons for delay.

Right of Access (2/3)

- Data controller must provide individuals with this information following an access request:

Information	Directive	GDPR
Confirmation as to whether data are processed	✓	✓
Purpose(s) of the processing	✓	✓
Categories of personal data processed	✓	✓
Categories of recipients	✓	✓ in particular data recipients outside EU
Data retention period / criteria used to determine this period	N/A	✓
Existence of a right to rectification, erasure, restriction or objection	✓	✓ (emphasis on right to object)
Right to lodge a complaint with DPA	N/A	✓
Source of the data	✓	✓
Existence of automated decision making and meaningful information about: • logic involved; • significance and envisaged consequences for individual.	✓ only re: logic involved	✓
Safeguards for data transfers outside the EU (if relevant).	N/A	✓

Right of Access (3/3)

- **In Practice?**
  - Controllers must provide more information than under Directive when replying to access requests.
  - Processors should not reply directly to access requests as this is the prerogative of controllers, but may want to consider implementing tools to allow controllers to comply with their own obligations:
    - Allow controller to obtain copy of all personal data relating to one individual, in a format that is intelligible for both the controller and the individual.
    - Implement access request handling procedure to follow-up on requests from customers.
- **How to Get Ready?**
  - Review your access request handling processes and procedures.
    - Assess need to redact or withhold documents to protect rights of others.
    - Provide contact details in easily accessible privacy policy.
  - Consider self-service platform for individuals.
  - Allocate responsibility and do staff trainings.

Right of Rectification & Right to Object (1/2)

- Broadly similar to the Data Protection Directive.
- Right to rectification:
  - Individuals have the right to obtain:
    - rectification of inaccurate personal data; and
    - completion of incomplete personal data where appropriate.
  - Obligation to communicate rectification to data recipient to whom the data have been disclosed.
- Right to object:
  - Legal ground for the processing is important!
  - Applies only when the data processing is:
    - based on the legitimate interests of the controller; or
    - necessary for the performance of a task carried out in the public interest.
  - Request must be granted unless the controller can rely on another legal ground:
    - controller demonstrates that there are compelling legitimate grounds that prevail, or
    - the processing is necessary for establishment, exercise or defense of legal claims.
  - Absolute right to object to direct marketing.

Right of Rectification & Right to Object (2/2)

- **In Practice?**
  - GDPR strengthens these rights, but no major change compared to the Directive.
- **How to Get Ready?**
  - Review your processes and procedure for allowing individuals to exercise their rights of rectification and to object to the processing.
  - Inform individuals of their rights in your privacy notice.
  - Provide means for requests to be made electronically (e.g., email address in privacy notice, opt-out links).
  - Implement automated process for handling direct marketing opt-out requests and opt-out lists.
  - If acting as a processor, consider allowing controllers to manage different opt-out lists per data processing purpose.

Right to Restriction (1/2)

- Broadly similar to current right to blocking.
- Intermediary step before deleting the data; put the processing on hold.
- It applies where one of the following conditions applies:
  - accuracy of the data is contested over a certain period of time;
  - processing is unlawful and the individual opposes the erasure of the data and requests restriction instead;
  - controller no longer needs the data for the purposes of the processing but the individual wants to maintain the data for the exercise or defense of legal claims; or
  - individual exercised right to object and the controller is in the process of verifying whether its interests override the interests of the individual.
- Examples of practices to restrict data:
  - temporarily move the selected data to another processing system.
  - make the selected data unavailable to users.
  - temporarily remove published data from a website.
  - flag the data in the in the IT system.

Right to Restriction (2/2)

- Communicate the restriction to data recipient.
- Data that is restricted may not be further processed in an active manner, but it may still be stored.
- When data have been restricted, they can only be processed in limited situations:
  - with individual's consent;
  - for the exercise or defense of legal claims;
  - for the protection of rights of another individual or organization; or
  - for reasons of important public interest of the EU or EU country.
- Before lifting the restriction, inform individuals.
- **In Practice?**
  - GDPR strengthens current right of blocking that was rarely used in practice.
- **How to Get Ready?**
  - Review internal processes e.g., implement process to flag data in the system so that they are automatically excluded from further data processing.
  - Reach out to IT department to strategize on how to comply with this right.

Right to Be Forgotten (1/2)

- GDPR builds on the right to erasure and codifies RTBF recognized by CJEU in *Costeja*.
- Essence: individuals have the right to obtain the erasure of their data.
- It is not an absolute right.
  - It applies upon individual's request when:
    - data are no longer necessary;
    - individual has withdrawn consent, and there is no other legal ground for the processing;
    - individual objects to the processing, and there are no overriding legitimate grounds for the processing, or individual objects to the processing for direct marketing purposes;
    - processing has been unlawful;
    - data must be erased in order for the controller to comply with a legal obligation; or
    - processing relies on child's (and / or parental) consent to information society service.
  - Controller can deny request if data is necessary for:
    - freedom of expression and information;
    - compliance with legal obligation (but only arising from EU or Member State law);;
    - performance of task carried out in public interest or exercise of official authority;

Right to Be Forgotten (2/2)

- reasons of public health;
- archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes; or
- establishment, exercise or defense of legal claims.

- Inform other data recipients to erase data (unless this would be unreasonable, taking into account the available technology and costs).
- **In Practice?**
  - GDPR makes clear that this right applies to all controllers (not only search engines).
- **How to Get Ready?**
  - Assess how individuals can exercise this right taking into account your business model.
  - Identify whether any processes can be automated.
  - Allocate resources to handle requests.
    - Consider that individuals may want to challenge your decision.
  - Stay up-to-date by monitoring WP29, EU Commission and EDPB guidance, national and CJEU case law.

Right to Data Portability (1/3)

- New right intended to enhance user choice and interoperability between online services.
  - Competition law rationale.
- Essence: individuals have the right to receive the personal data that they provided to a controller, and transmit those data to another controller.
  - If requested by an individual, the controller must transmit the data directly to another controller, "where technically feasible."
  - Without hindrance from the controller.
- This is not an absolute right; it only applies in limited situations:
  - when processing is based on individual's consent or is necessary for the performance of a contract; and
  - only for processing carried out by automated means.
- Data must be provided in a structured, commonly used, machine-readable and interoperable format.
  - But this right should not create an obligation for controllers to adopt or maintain processing systems that are technically compatible.

Right to Data Portability (2/3)

- Right to data portability v. other rights:
  - Right to data portability cannot adversely affect the rights and freedoms of others (e.g., when more than one individual is concerned).
  - Right to data portability is independent from the right to be forgotten / right to erasure.
    - Data portability as such does not require controllers to erase the data.
    - In particular, if the data are necessary for the performance of a contract, this right should not imply the erasure of that data.
- Examples of data which could be affected:
  - Browsing history.
  - Transaction history.
  - Social network data.
- Guidance on data portability is one of the priorities for WP29 this year.

Right to Data Portability (3/3)

- **In Practice?**
  - You may be requested to extract the data that a user provided to you, and, where technically feasible, transmit it directly to your competitor.
  - Data portability concerns only the data that have been provided to the controller by the individual in question. It does not concern, e.g.:
    - Data provided by others about this individual.
    - Data produced by controller.
  - This right does not apply when processing is based on different legal basis than individual's consent or performance of a contract.

- **How to Get Ready?**
  - Assess whether you should put in place new or updated processes, procedures and IT systems to allow data portability.
  - Inform individuals of their data portability right in a privacy notice.
  - Monitor WP29 guidance.

Exceptions to Individuals Rights

- The controller doesn't need to satisfy individual's requests if it proves that the individual cannot be identified:
  - No obligation to maintain, acquire or process additional information to identify individual, if the purposes for which controllers process data do not or do no longer require the identification of individuals.
  - If possible, the controller must inform the individual that it cannot identify him or her.
  - But if the individual provides additional information enabling his or her identification, the controller cannot refuse to act.
  - Identification may be digital and take place through authentication mechanism (e.g., the same credentials used by the individual to log in to the controller's online service).
- National law can restricts the rights for a number of important public interests, which create a risk of fragmentation.

Right Not to Be Subject to Automated Decision Making (1/3)

- GDPR strengthens this right and clarifies that it applies also to profiling resulting in automated decisions.
- Lot of uncertainty around the exact scope of this provision and its impact on certain activities (e.g., OBA).
- Prohibition: Individuals have the right not to be subject to a decision based **solely** on automated processing, **including profiling**, which produces **legal effects or similarly affects** that individual.
  - Potential examples of activities captured by this provision: e-recruiting, credit scoring, price discrimination.
- Profiling means evaluating certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- Profiling activities must comply with general data protection rules, including ensuring fair and transparent processing by :
  - using appropriate mathematical or statistical procedures;
  - implementing measures to ensure that inaccuracies are corrected and the risk of errors is minimized;
  - preventing discriminatory effects on individuals.
- Restricted legal grounds to carry out automated decision making:
  - entering into, or performance of contract;
  - EU law or national law (including for fraud and tax-evasion monitoring and prevention); or
  - explicit consent.

Right Not to Be Subject to Automated Decision Making (2/3)

- If sensitive data are involved, only allowed if legal ground is :
  - EU law or national law; or
  - explicit consent.
- There should be safeguards :
  - individuals must have at least the right to:
    - obtain human intervention;
    - express their views;
    - obtain explanation of the decision; and
    - challenge the decision.
  - mandatory PIA (and DPO in certain situations)?
  - information in privacy notice and upon individual's request to access the data.
  - implement measures to ensure that inaccuracies are corrected, risk of errors is minimized and data are kept secure e.g., to prevent discrimination (e.g., based on racial profiling).
  - prohibition of automated decision concerning children.
- Once established, EDPB may issue guidance on profiling.

Right Not to Be Subject to Automated Decision Making (3/3)

- **In Practice?**
  - Stricter conditions for automated decision making.
  - More transparency required.
  - Profiling activities are captured by this provision only if they produce legal (or similar) effects
- **How to Get Ready?**
  - Identify processing activities that result in automated decisions producing legal effects or significantly affecting individuals.
  - Ensure some degree of human intervention in decision-making process (e.g., avoid e-recruiting practices without human intervention, automatic refusal of an online credit application).
  - Adopt processes to allow individuals to exercise their rights related to automated decision-making.
  - Review privacy policy to ensure individuals are sufficiently informed.
  - Conduct PIA and document it.

Data Breach Notification (1/2)

- Introduction of new data breach notification requirements:
  - Data breach = breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

DPA Notification	Notification to Individuals
Without undue delay, within 72 hours. If submitted after, must include justification for such delay	Without undue delay.
Breach that presents risks. It's up to controller to demonstrate that data breach is unlikely to result in risks (accountability principle).	Breach that presents **high risks**.
Nature of the breach, DPO / contact point, likely consequences, measures taken to address the breach, measures to mitigate adverse effects .	DPO / contact point, likely consequences, measures taken to address the breach, measures to mitigate adverse effects. Notification must be in clear and plan language.
No exception.	Encryption (unintelligible), measures to mitigate high risks, or disproportionate efforts.

- Processor notification: to controller, without undue delay.

Data Breach Notification (2/2)

- **In Practice?**
  - General data breach notification requirement imposed on all controllers, sector-wide.
  - Incentive to secure personal data.
  - Will coexist with breach notification requirements under NIS Directive.
- **How to Get Ready?**
  - Prepare new or assess existing data breach response plan.
  - Encrypt personal data, or implement other security measures, to ensure that data are unintelligible in case of data breach.

Conclusions

- GDPR is built on the same core principles as the Directive, but it enhances individuals' rights and introduces new ones. This means new obligations for controllers!
- Processors will be indirectly affected as well:
  - Controllers will require processors to implement appropriate technical measures.
  - Processors should build products and services in a way that allows controllers to comply with new obligations.
- The GDPR is a game-changer; enforcement risk will be much higher.
- Stay up-to-date: monitor upcoming regulators' guidance and CJEU decisions.
- Use the 2-year transition period wisely.
- Changing practices takes time and should be planned in advance.
- **Stay tuned for our next webcasts!**

The GDPR for service providers: New obligations, contractual provisions, sub-processing	**July 12**
International data transfers under the GDPR	September
Regulatory aspects of the GDPR: DPAs' powers, the EDPB, the one-stop shop, recourse mechanisms	October
A panel discussion with leading privacy officers on how to get ready for the GDPR	November

Questions?

Thanks!

Cédric Burton
Of Counsel
cburton@wsgr.com

Laura De Boel
Senior Associate
ldeboel@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.
- C. Burton, L. De Boel, S. Cadiot and S. Hoffman, *New EU Data Protection Regulation Is Now Enacted*, WSGR Alert, April 14, 2016.
- C. Burton, L. De Boel, C. Kuner, S. Cadiot and S. Hoffman, *The Final European Union General Data Protection Regulation*, BNA, January 25, 2016.
- C. Burton, L. De Boel, C. Kuner, A. Pateraki, *The Proposed EU Data Protection Regulation Three Years Later: The Council Position*, BNA June 29, 2015.
- C. Burton, C. Kuner, A. Pateraki, *The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report*, BNA, January 21, 2013.
- C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BNA, February 6, 2012.