What is it and what to do?

Simon.Hania@tomtom.com

Narrative is in speaker notes!

European Union General Data Protection Regulation

An evolutionary upgrade and unification across the EU of laws from the previous century

- Applies across the entire European Union as of 25 May 2018
- Existing national laws are repealed
- GDPR applies to those taking decisions regarding personal data use:
  - anyone from anywhere who targets people in the EU and uses their data
  - anyone from the EU who uses personal data from anywhere
- New and expanded elements:
  1. Accountability – tell what you do, do as you tell and be prepared to prove it
  2. Stronger rights for individuals: “right-to-be-forgotten” & data portability
  3. Must do: data protection impact assessment and data protection by design
  4. Expanded documentation and explanation duties
  5. Security failure & data breach notification obligations
  6. More than 40 independent national & regional supervisors will provide a consistent one stop shop to citizens and businesses
  7. Worst case fines of upto 4% of global annual revenue for businesses

Personal Data

- Contains (whatever) information relating to a natural (“real”) person
- That person could be identified, directly or indirectly
- Typically: data attached to unique identifiers

- Anonymous only:
- When no reasonable way exists to identify (or “single out”) a person
- Even when requiring correlation with other data sources (e.g. maps and phonebooks)
- By anyone with the right resources
- Unless clearly to much effort or cost

Typical personal data misconceptions

very often present in technology companies

- We do not identify the user while using the data, so we have no issues with privacy law
- We only use the serial number of the users device, so the data is anonymous and we have no issues with privacy law
- We encrypt the data, so we are no longer using/receiving/sending personal data
- We use hashes to replace all serial numbers, so the data is now anonymous and we have no issues with privacy law
- We anonimize the data, so we are not using personal data
- We can use the users' data for anything we want, as long as we keep the data to ourselves
- Look: big name companies are doing the same, so we are OK

Key elements of EU GDPR

Best considered as engineering requirements

1. Applies to all Personal Data
2. Pre-defined, specific purposes only
3. Kind, volume and time limitations
4. Understandable explanation in advance
5. Permission, execution of a contract/delivery of a service, legal obligation or demonstrable prevailing legitimate interests must apply
6. Undeniable right to view, correct, object, erase and download/transfer
7. Protect confidentiality, integrity & availability with TOMs

What must be in place for GDPR

Ten key objectives to achieve, be able to prove and be accountable for

1. Data protection by design and by default
2. Up-to-date data inventory: what, why, who, when, where
3. User friendly explanations regarding data use
4. Be able to allow access, correct, block, erase, download & transfer
5. Technological and operational up-to-date security measures
6. Detection, correction, recording and notification of security failures
7. Contracts with all suppliers touching personal data: do-as-we-tell
8. Automated decisions and profiling adhering to strict conditions
9. Prior assessment and mitigation of privacy risks to individuals
10. Effective data protection officers/coordinators

Data protection by design and by default

best embedded in engineering workflows

Designing or implementing new services or systems requires demonstrable and documented data protection by design.

This must be based on assessment of

1. state of the art
2. cost of implementation
3. nature, scope, context and purposes of processing
4. risks to the individuals concerned (severity and likelihood)

By default data processing must be minimized in terms of volume, time and exposure of the data.

Data inventory

Continuous, complete and accurate overview of

1.	What	Categories of data and their meaning
2.	Why	Purposes & legal bases spelled out
3.	Who	Categories of individuals concerned
4.	Who else	Categories of recipients or third parties
5.	When	Data erasure time or criteria
6.	Where	What database/system and jurisdiction
7.	TOMs	Technical and organizational security measures

Define and describe all personal data

- Data elements + semantics
- Grouping into categories is possible to avoid the need to give too much detail
- Examples are:
    - “orders”
    - “map corrections”
    - ”gps traces”
    - ”name/address information”
    - “MyTomTom account”
    - “diagnostic data”,
    - “individual site usage events”

Define and describe purposes

- A purpose describes why the data is processed (“if you cannot explain it, you probably shouldn’t be doing it”)
- A purpose needs to be specific, well-defined and comprehensible for an average user without expert legal or technical knowledge
- Examples are “delivering the traffic service”, “sending an email news letter”, “generating and applying user profiles to tailor offerings”, “improving our products and services, after anonimisation”
- Examples of not well-defined purposes: “marketing purposes” or “service improvement”: too unspecific
- Categories of data can have multiple (separate) purposes

Rightsize on volume and time

- Purely based on purpose:
  - Can we achieve the purpose in other ways?
  - How much is needed? Can we do with less?
  - How long do we need it? Can we do with less?

- When can we destroy the data??
- What triggers destruction? Time, events?

- Anonimisation instead of destruction is a way to lift volume and time limits
- Aggregation and destruction is a way to lift volume and time limits (provided the aggregate is non-personal)

Establish potential for pseudonimisaton, anonimisation, aggregation

- Pseudo-anonimisation, anonimisation & aggregation are processing of personal data and require correct legal basis

- Pseudo-anonimisation can serve to tip the balance in case of “legitimate balance”, by reducing the “interference level”

- Anonimisation & aggregation result in data to become non-personal and hence privacy law to become no longer applicable

Using pseudonyms a.k.a. aliases

It’s like a proxy firewall for data, providing context separation, potentially improving privacy – but beware, many variations exist

- Pseudonyms replace identifiers with newly generated identifiers (“alias”)
- The mapping between identifier and pseudonym/alias is kept confidential and only accessible to the entity replacing the identifiers
- This reduces possibility for re-identification to the entity receiving pseudo-anonymous data, reducing privacy risks by making the data “less personal”
- The possibility of re-identification can be a welcome asset of pseudonyms: e.g. in medicine research in case of (life threatening) issues
- In other cases pseudonyms are an intermediate step towards true anonimisation or aggregation: here being able to revert or “crack” a pseudonym is a liability
- Various mechanisms for generating a mapping exist: random number generation + look-up tables, reversible encryption, “non-reversible” hashing etc: the mechanism impacts the level of “less personal”
- Pseudonym lifetime (i.e. pseudonym destruction or re-generation) is highly relevant in assessing re-identification potential: shorter lifetime reduces re-identification potential
- For controller-controller transfer, consider double pseudonimisation:
  each entity inherently in control over identifiers used

Data inventory

Legal bases – select one out of six conditions for lawful processing

1. Consent
   Informed, freely given, withdrawable, clear affirmative action, default off, demonstrable

2. Contract
   Necessary to enter into or to execute against (service) contract

3. Legal obligation
   Necessary to satisfy obligation from EU/MS law (not: foreign!)

4. Vital interest
   Only in life/death situations and incapacity of individual

5. Public interest
   Necessary to carry out public task by government bodies only

6. Overriding legitimate interest
   Necessary to satisfy a legitimate interest that overrides right of individual to ”be left alone”. Reasoning must be documented and impact to individuals’ freedom and level of self determination clearly must be minimal.

Explaining data use to the individuals concerned

Must be a user friendly explanation not unlike a user manual

1. Who is responsible and accountable
2. What data is being used and how long the data is kept
3. Purposes and legal bases spelled out
4. Description of the legitimate interests (if applicable)
5. Recipients and third parties all listed
6. Transfer out of the EEA (if applicable) plus safeguards in place
7. Point out individuals' rights (view, correct, block, erase, download/transfer, object, complain)
8. If applicable: point out statutory or contractual requirement compulsory nature and consequences of not providing
9. Explanation of automated decision making including profiling
10. Same for any use beyond original reason for collection

Users have rights and you need to be able to honor them

Each individual must be able to:

1. Access/view his data
2. Obtain a (hard-)copy of all of his data
3. Have his data corrected upon request
4. Have his data erased, if one of the conditions in GDPR apply
5. Have is data made read-only e.g. in case of disputes
6. Obtain an electronic download of user contributed data and transfer to someone else, if conditions in GDPR apply
7. Be able to object to further processing

Ensure date is deleted if there is no use for it anymore

- “End-of-life” data must be irreversibly deleted (or anonimised)
- Putting data in “stasis” (archive) is acceptable provided it remains there
- Destroying encryption keys on strongly encrypted data also is a way to “end-of-life” data
- Consider how this affects back-up and especially recovery scenario’s

Data portability (download, export, import, share)

- Right applies in case of automated means & consent or contract

- Receive data provided & transmit to another without hindrance
- Transmit directly to another where technically feasible

- Structured, commonly used, machine readable format
- Interoperable format (as mentioned in recital)

- Consider rights and freedoms of others
- Consider right to erasure independently

Security

Technological and operational security measures – an ongoing effort

Technical and operational measures must be in place considering:

1. state of the art
2. cost of implementation
3. nature, scope, context and purposes of processing
4. risks to the individuals concerned (severity and likelihood)

Objective: prevent risks arising from unauthorized or unlawful

1. destruction
2. loss
3. alteration
4. disclosure
5. access while transmitted, stored etc.

Personal data breaches = failed security measures

Document and notify to authorities based on severity

Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

- All breached must be documented internally
- Notification to authority in case:
  - Likely resulting in risks to the individuals concerned
  - Prompt notification, no later than 72 hours, must include:
    - Nature of breach, number of individuals, categories and volume of data
    - Likely consequences
    - Measures taken including mitigation of adverse effects

Personal data breaches = failed security measures

Communication to individuals

Prompt notification in plain language, same info as to authorities in case the personal data breach:

- Likely results in high risks to the individuals concerned

Notification is not required in case:

- Strong encryption is in place and keys are still secure or
- Measures exist to mitigate subsequent adverse effects or
- Individuals cannot be easily reached (in that case: public communication/announcement)

Data contract with suppliers

Particularly: “data processors”

1. Strictly abide by instructions regarding acceptable data use and warn in case of suspected illegal instructions
2. Staff involved must all be under NDA
3. Security of processing must remain arranged according to specification
4. Only use subcontractors with prior approval, meeting identical requirements
5. Assist with adhering to individuals’ rights
6. Erase or return all data at end of contract
7. Provide all information to demonstrate compliance
8. Allow inspections and audits as mandated
9. Fully and timely cooperate with respect to data breaches

Execution of impact assessments

Data processing impact assessment required if:

- New technologies or high risks to individuals' freedom
- Evaluation/assessment of individuals based on automated decision making with legal or significant effects
- Large scale processing of amongst others health or criminal data
- Systematic monitoring of public places

Data processing impact assessment contains at least:

- Thorough description of how the processing will be conducted and the purposes, including the legitimate interest pursued
- Assessment whether alternative or less intrusive options exist
- Assessment of the risks to the individuals rights and freedoms
- How these risks will be mitigated in compliance with law

Thank you

Any questions?