Sirius Legal

GDPR en databescherming in een smart city context

Master Class: Smart City Data & Privacy, Brussel 6 september 2018
1. We live in a digital world…

Basis of anything that happens online is data
Big data
Collect all you can now – figure out what to do with it later
Profiling
Maximale tracking
Location based
Trigger based
Internet of things

Data has in many cases become a currency online…
1. In a smart city context…

Barcelona - London - Hamburg - Singapore - Dubai - Boston - ...

Smart city projects multiply at great speed

Traffic management
Waste management
CCTV security camera’s
Access control
Public lighting
Smart information panels
Smart infrastructure (swimming pool, fire security, central heating systems in public housing, ...
1. In a smart city context...

Barcelona - London - Hamburg - Singapore - Dubai - Boston - ...

Smart city projects multiply at great speed

Often based on, or related to

Internet of Things
Big Data processing
A certain degree of profiling
Cloud storage / use of public internet for data transportation
Public-Private Cooperation
2. Same rules for all and no grace period…


Entered into force last May 2018 (without grace period!)

New rules are MUCH stricter than current law and impact EVERYONE present here today

Be prepared: high fines – liability – insurance issues – company image
3. Everybody collects personal data…

GDPR applies to ALL databases (clients, marketing, sales, HR, purchasing, accounting, ...)

Personal data = **EVERY** piece of information that allows you to identify a person, directly or indirectly, now or in the future, alone or with the help of third parties

Compliance is mandatory not only for “Data controller” (e.g. the advertiser) but in many cases also for “data processor” (e.g. cloud service provider, web developer, online agency, etc...)

Specific caution is required for all data driven innovation – apps – AI – location based – blockchain – IoT - ...

Marketing – HR – sales – purchasing – reception – call center – IT - ...
3. In a smart city context...

Distinction to be made between

Aggregate data
Traffic streams, number of visitors, crowd management, ...
Pseudonymised, anonymised, no longer personal data
But risk related to big data = retroactive (even unintended) de-pseudonymisation

Real time data
NPR, CCTV, MAC and IP addresses, facial recognition systems
All processing of personal data
Great number of privacy related issues
4. Basic principles of GDPR to learn by heart…

Accountability
Transparency
Data Protection by design
Data protection by default
Purpose limitation
Data minimisation
Accuracy
Limited retention time
Data security
Limits on data export outside EU/EEA
Access on need to know basis only
4. Challenges in a smart city context…

Transparency

Cfr. CCTV, facial recognition, profiling, ANPR, ...

PPC - sharing data with private companies

Democratic and legal risk of loss of transparency towards citizens
4. Challenges in a smart city context…

Data Protection by default / by design

Necessity to make full scale DPIA a standard reflex

Ensure both technical and operational security

Ensure correct application of principles of transparency, minimisation, limited retention times, purpose limitation, data security, access at need to know basis

Data protection by design: problem of third party software / off the shelf software that is not always compliant
4. Challenges in a smart city context…

Purpose limitation

Quintessential issue related to big data is that purpose of data collection is often unknown at the time of collection.

Tempting to reuse data for new purposes that present themselves post factum.

Cfr. legal basis for processing + transparency.
4. Challenges in a smart city context…

Data minimisation + limited retention times

Cfr. ANPR - CCTV - MAC and IP addresses - Facial recognition

Only data that is absolutely necessary for successful service can be processed
Only for the time required to provide successful service

“Need to know” - “need to process”
4. Challenges in a smart city context…

Data security

Potential issues with data security are related to

Poor security on devices / sensors (cfr. baby monitoring hacking)
Poor security on networks (cfr. highjacking of Jeep Cherokee in 2015)
Out of date technology
Cloud storage
Sharing with third parties
Insufficient organisational security (access control to buildings, password security,...)
4. Challenges in a smart city context…

Data export outside EU/EEA requires safe country, standard clauses, BCR, US/EU privacy shield, ...

Any “export” outside these conditions is illegal

Potential risks
Cloud storage (location of data centers)
Use of non-EU software or IT service providers
PPC with non EU partners or EU partners with non EU subcontractors

...
5. Contracts with all contractors...

Obligation to work only with subcontractors that guarantee sufficient data security
Obligation to have written contracts with all subcontractors
List of mandatory clauses in such contracts

Also concerns software tools...
= Need to audit/map all existing subcontracting/service contracts/licenses (Mailchimp, Eventbrite, (Google) Analytics, internal messaging (e.g. Slack)...°
6. Everything starts with a data register

Obligation to maintain a “record of processing activities”
Holding ID of processor, processed data, categories, transfers, time limits, security measures
In writing at the seat of your company
Privacy Commission has a template (rather complicated), so do we (simplified)

Bookings, mailings, transfers to third parties, opt-outs, ...
7. What is “Appropriate” Security…?

“Processor shall implement appropriate technical and organizational measures, to ensure an appropriate level of security”

Pseudonymisation where possible, confidentiality, security, back ups in place, security testing protocols, ...

= Need to audit/map data within company
7. Appropriate security in a smart city context…

Potential risks from a technical perspective
Hacking and theft of personal data
Cryptolocker / ransomware attacks on personal data files (or on smart city services!)
Loss of personal data due to e.g. power outage, lack of back up, etc...
Highjacking of IoT networks as part of botnet

Potential risks from a privacy perspective
Unlawful sharing of data with third parties (PPC partners?)
Unlawful access (“need to know basis only”)
Abuse of IoT by government itself or as part of third part hacking to illegally collect data
De-pseudonymisation of data
Unlawful repurposing of data
7. Appropriate security in a smart city context…

What is appropriate security

Necessity to conduct DPIA
Ensure Data Protection by Design and Data Protection by Default
Very strict Data Processing Agreements with all contractors
Clear Data Security Policy (dataveiligheidsplan) within organisation
Strong DPO (+ independant Informatieveiligheidsconsulent)
White hacking as essential part of data security
Strong internal policies towards employees - BYOD - Homework - visitors - password security - ...
Access control, device management - swiping and blocking - Data Use monitoring - ...
Data breach notification policy
Awareness training
8. Find processing grounds for ALL records...

1. Legal interest – (2. vital interest) – (3. Public interest)
4. Prior opt-in remains the basic rule (+ proof required)
5. “Processing is required for the execution of a contract”
6. “Legitimate interest” (risky business...)
8. Processing grounds in a smart city context…

Prior opt-in should be basis if and when possible

Reality in smart city / IoT / Big Data context is that opt-in is an illusion

Cfr CCTV - NPR - Facial recognition

Cfr eg Singapore where proposal is to use geolocalisation device for every car or to start large scale monitoring of energy use in public housing on individual level

“Legal obligation” will very often be legal ground for processing

“Execution of a contract” may in some cases be sufficient ground (but not if there is no “contract..” and not if not “needed” to perform contract

What is left is “legitimate interest” (not for “public authorities” in the “performance of their task”??)

Sliding scale! - Should be limited to those cases where opt-in cannot be obtained and with very big auto-restriction
Processing of data belonging to minor (-13 Y/O, -16 Y/O)

Always requires explicit authorisation by parents!

“Reasonable efforts” to check age and obtain authorisation

eID?, Facebook login?, credit card data?, live chat, ...?
10. Information, information, information…

In all circumstances

ID processor, rights of data subjects, type of processing, ...

Specifically in case of
Data transfer
Data export
Minors
New processing grounds
Profiling & automated decision taking
...
10. Information obligations in a smart city context…

How to...

Give information prior to processing when processing occurs automatically?

Give information on profiling and allow opt-out for profiling?

Give access to data and allow correction of data?

Inform on sharing of data with third parties?

...?
GDPR in a smart city context…

In conclusion

GDPR in a smart city context

Raises more questions than answers
Requires thorough legal analyses and professional guidance
Non respect of GDPR poses a real risk for democratic deficit
Non respect of GDPR poses a real risk of serious damage to brand image
Very high fines
Series of other invasive sanctions (halt to processing, suspension of processing, etc...)
Sirius Legal

Media & advertising law
IP law
Internet & e-commerce
Privacy & Data Protection
Gambling law
Travel & consumer protection
Commercial & contracts
Corporate - tax - labour - real estate

bart@siriuslegal.be
www.siriuslegal.be
@BartVdBrande
Linkedin.com/in/bartvdb