TOP 10
Benefits of the GDPR

(for hackers)

„as kind of lightning talk“

Created by Grete DV GmbH 2018 - created for **EU EDPS IPEN. Copy** and disclosure allowed.

Motivation

When you are out there, doing GDPR, installing systems, doing consulting, creating concepts
… and still remember your times in ***IT-Security***…

Sometimes there is a little ***headache***.

I got the Idea of writing about
"***10 different benefits*** of the GDPR for ***hackers***".
I was sure by the first moment I will find 10 just out of my headache.

Here they are.

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

My “TOP 10 BENEFITS” of the GDPR (for hackers)

1. Centralized „**data access rights**“ systems are installed
2. More **data** is accessible due to an increase in digitalization
3. Higher **sum** of IT privacy & security **costs** due to the GDPR
4. Rising system **complexity** due to more connections
5. Enhancement of **social engineering** due to uncertainty
6. Falling average **knowledge** of IT-security „experts“
7. New **legal destruction** patterns against SMB-companies
8. Data is **coming back** to the European Union
9. Hackers are **cool** right now
10. EU regulations are “**interpretable**”

1. Centralized **„data access rights“** systems are installed

Contradiction in the mindset:

- The GDPR requires the best „**separation of data**“ as to „privacy by design“.
- The GDPR grants „data access rights“ to „**all data**“ considering a data subject

Resulting problem:
No matter whether an ESB or a DWH is used for the “data access rights“
– there is a „easy to use“ way right now.

Benefit for Hackers:
„**simple points of attack**“ / Hackers do not need to collect all the data

Good for:
bad hackers, state hackers

Solution:
E.g. customers key – as in bank safes, the clerk has one and the customer has one.

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

2. More **data** is accessible due to an increase in digitalisation

Contradiction in the mindset :

- due to „privacy by design and default“ the amount of data collected accessible must be minimized
- due to the „data access rights“, data on any kind of filesystem is affected and has to be offered, so more and more data is digitalized. Data which has not been accessible without big efforts in the past, is now available.

Resulting problem:
The amount of easy accessible data is increasing without increasing the overall amount of data collected.

Benefit for hackers:
A bad hacker gets more data (more value on the market for him)

Good for:
bad hackers, state hackers

Solution:
No Solution. Digitalization will come anyway. We are just getting it faster by GDPR

3. Higher **sum** of IT privacy & security **costs** due to the GDPR

Contradiction in the mindset :

- The GDPR is set kind of „on top“ of IT-Security with GDPR article 32. That means that the same persons as before (CISO, CRO, CFO, CEO) are in charge for more tasks, parts of then involve strong digitalization costs, staff costs for call centers etc.
- The GDPR does not enhance possibilities for more money to companies. So the purses of the man in charge are not filled higher by processes of the market. They have to get a huger share from the other departments without delivering more value to the company (no zero-sum as it should be)

Resulting Problem:
The amount of money which can be spent is watched twice and each new measurement is evaluated very carefully concerning resulting costs.

Benefit for hackers:
The level of it security is falling, as the purses have to be shared with privacy business processes

Good for:
bad hackers, state hackers

Solution:
EU should start awarding e.g. “privacy stars” for cool implementations – returns money on privacy

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

4. Rising system **complexity** due to more connections

Contradiction in the mindset :

- data quality is an aspect of data protection. so all deletions and blockings of data must be forwarded to data recipients, changes on parts of data should be forwarded. Data subjects have the right of data portability
- there is no common infrastructure for secure data transfer and no common semantic framework for data processing in 2017 or middle of 2018

Resulting Problem:
The **right for data portability** leads to an rise in networking between companies, as companies have to construct a secure infrastructure for transferring parts of personal data (which was handed in before) without any given unionwide framework

Benefit for hackers:
Rising system complexity and network complexity leads to more mistakes / open backdoors.

Good for:
bad hackers

Solution:
The sematic web and many ontologies are already known. There should be a common infrastructure.

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

5. Enhancement of **social engineering** due to uncertainty

Contradiction in the mindset :

- All staff of all companies has to be well informed about the GDPR, about the data subject rights, about the design principles, about the corresponding legal issues
- The companies are already in trouble with implementing digitalization. Rules are not as strict as they should be. Even experts argue against each other. Consulting businesses partially do not consult due to the high risk if some results to be wrong

Resulting Problem:
The guys in the call centers are insecure. Even with good education, they are no lawyers. The risks are that they hand out data to persons not valid recipients (data access rights by falsified email address) or to hand out to few data just be being careful

Benefit for hackers:
Hackers can use social engineering now to get the data they want – and fast.

Good for:
bad (social engineering) hackers

Solution:
The GDPR is “not off the EU table” from 25.05.2018 on. Not only FB and Insta have to educate.

6. Falling average **knowledge** of IT-security „experts“

Contradiction in the mindset:

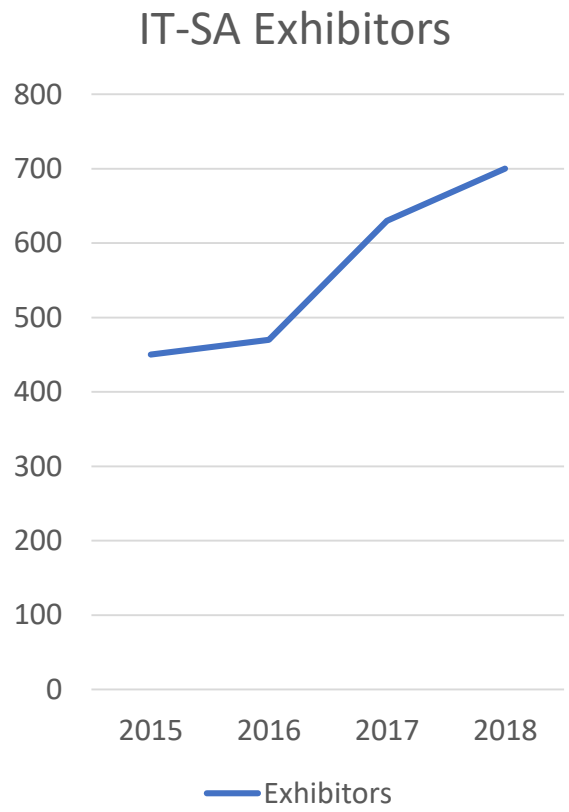
- We want more guys/gals doing IT security and IT privacy
- We do not have more of them

Resulting Problem:
People who have basic IT-Sec knowledge
are doing data protection consulting now.
The IT-SA fair in Nürnberg uses 3 times
more space in 2017 compared to 2014-2016.
Either we got 3 times the experts in one year,
or the overall knowledge level dropped dangerously.

Benefit for hackers:
The IT sec staff is missing in their original area, and the concepts are weak

Good for:
Bad hackers, state hackers

Solution:
The market will sort that out. Will take time



Source: IT-SA newsletters, www.it-sa.de

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

7. New **legal destruction** patterns against SMB-companies

Contradiction in the mindset:

- We want stability, good running businesses and clear rules in Europe
- We establish rules which have to be interpreted and have no clear ruling across Europe (not even across Germany). It will take years to get a leveraged understanding of the implementation of the GDPR.

Resulting Problem:
While it is not clear by 100% what companies really have to do, and there are not enough toolings and free of charge guidelines, specialized lawyers and companies will find their ways to bring harm to many companies.
I got input from **startups** that they have the fear about being extinguished by a bigger competitor “death by GDPR”.

Benefit for hackers:
Easy way to earn money with dissuasions / blackmailings in form of circular letters

Good for:
Legal company destructors / „Legal system hackers“

Solution:
There should be measurements against “privacy for privacys sake without zero-sum”
and special help and free-of-charge toolings for **smaller companies** and **startups**.

8. Data is **coming back** to the European Union

Contradiction in the mindset :

- GDPR requires separation of data
- Due to insecure concepts with other countries data has better to be stored inside the EU

Resulting Problem:
Data is less separated by location, country and law system.

Benefit for hackers:
State hackers of the member states of the European Union now have better access, because the data is no longer stored outside in „bad countries“

Good for:
State hackers of EU countries

Solution:
Well, the state hackers are the problem. So better encryption is the solution.

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

9. Hackers are **cool** right now (!)

Contradiction in the mindset:

- GDPR and IT security is put against hackers who steal data
- The GDPR would never have been enforced that fast, if there would not have been the case of Edward Snowden. However *you* call somebody who takes data he is not allowed to take it, and publishes it… I call those people ***hackers***.

Resulting Problem:
What is cool and good and what is bad right now?

Benefit for hackers:
Nobody knows

Good for:
Whistleblowing hackers, casual hackers

Solution:
Hackers should be declared evil again. Sorry, CCC.

10 EU regulations are “**interpretable**”

Contradiction in the mindset:

- The **GDPR** (Directive 95/46/EC) says in **article 5** the amount of personal data stored must be “**adequate, relevant and limited to what is necessary”** (data minimization).
  Hackers of today are usually natural persons. What is “adequate is up to the “experts”.
- **Directive 2016/1148** connects to GDRP in Article 2, but refers in **Article 14** to the “**state of the art**” on network security. Scientists, assessors and experts discuss what that could mean.

Resulting Problem:
As GDPR has high punishments, less data than necessary is stored due to insecurity and already ongoing court cases against storing of IP addresses (EuGH C-582/14 ➔ BGH VI ZR 136/13)

Benefit for hackers:
If they are caught, they sue the company for storing their data. If they are not caught, even better.

Good for:
All kinds of hackers.

Solution:
We need a regulation as §5 BSI law in Germany, which tells precisely what is allowed.
E.g. store protocol data for 3 month and do automated analyses on it as in SIEM systems which store “everything”.

Results

Please help getting the European Union a little more **save** and **enhance freedom**.
Please work on the **solutions** or **suggest better** ones.

Many thanks to

- the **L3S Research Lab** (www.l3s.de) for many inspirations,
- Prof. Dr**. Tina Krügel** (www.iri.uni-hannover.de) for discussions and inspirations,
- and finally the guys from the **DLR** (www.dlr.de) for affirmative support in discussions

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.

Thanks for the attention

For further inquiries / information please contact:

Markus Grete
Markus.Grete@gretEDV.de

Member of **IPEN**
which is the Internet Privacy Engineering Network
of the European Union / European Data Protection Supervisor

Created by Grete DV GmbH 2018 - created for EU EDPS IPEN. Copy and disclosure allowed.