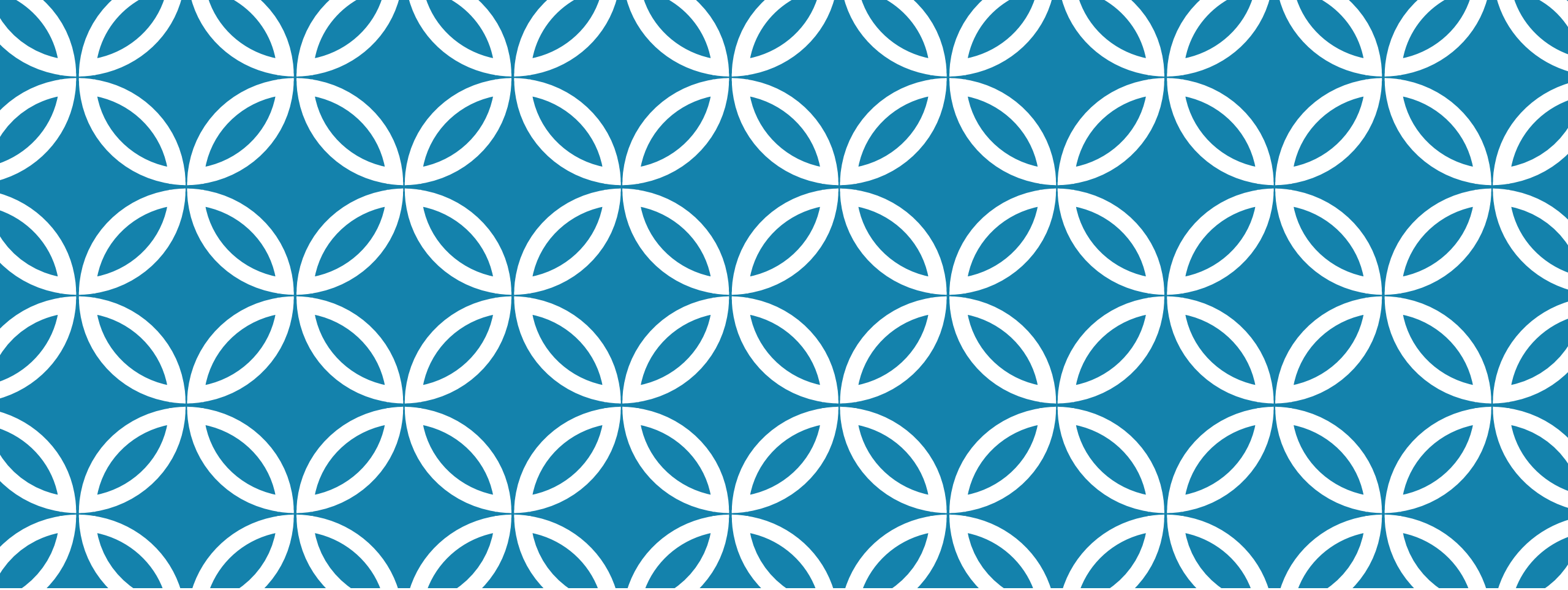


PRIVACY BY DESIGN AND BY DEFAULT -> GDPR

Peter Prochazka

26.06.2018

SUG Hungary - Budapest

HAVE YOU HEARD OF PRIVACY BY DEFAULT?

HAVE YOU HEARD OF PRIVACY BY DESIGN?

HAVE YOU HEARD OF GENERAL DATA PROTECTION REGULATION A.K.A GDPR?

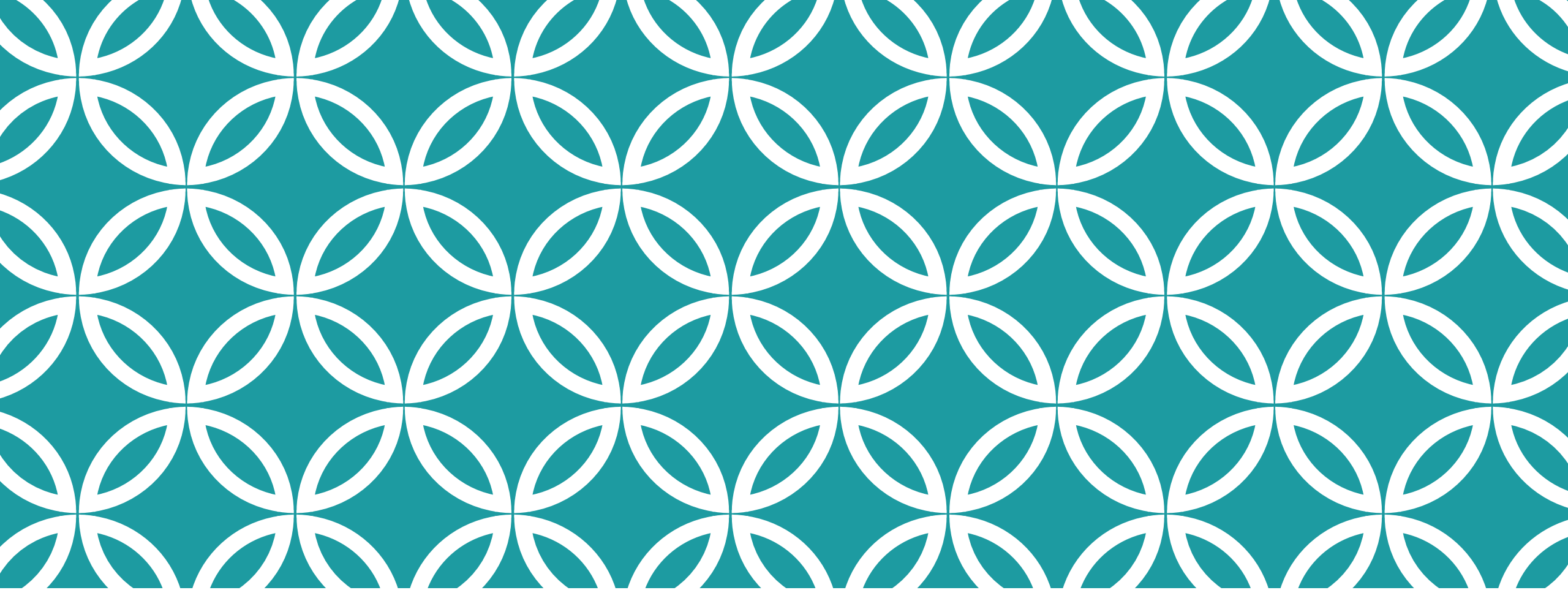
IT'S ESTIMATED THAT 90% OF THE WORLD'S DATA HAS BEEN COLLECTED IN THE LAST TWO YEARS.

BY THE YEAR 2020, IT'S EXPECTED THAT WE WILL CREATE 1.7 MEGABYTES OF NEW INFORMATION EVERY SECOND FOR EVERY HUMAN ON THE PLANET.


GDPR

AGENDA

- Privacy by Design & Privacy by Default
- General Data Protection Regulation (GDPR)



PRIVACY BY DESIGN & PRIVACY BY DEFAULT

PRIVACY BY DESIGN

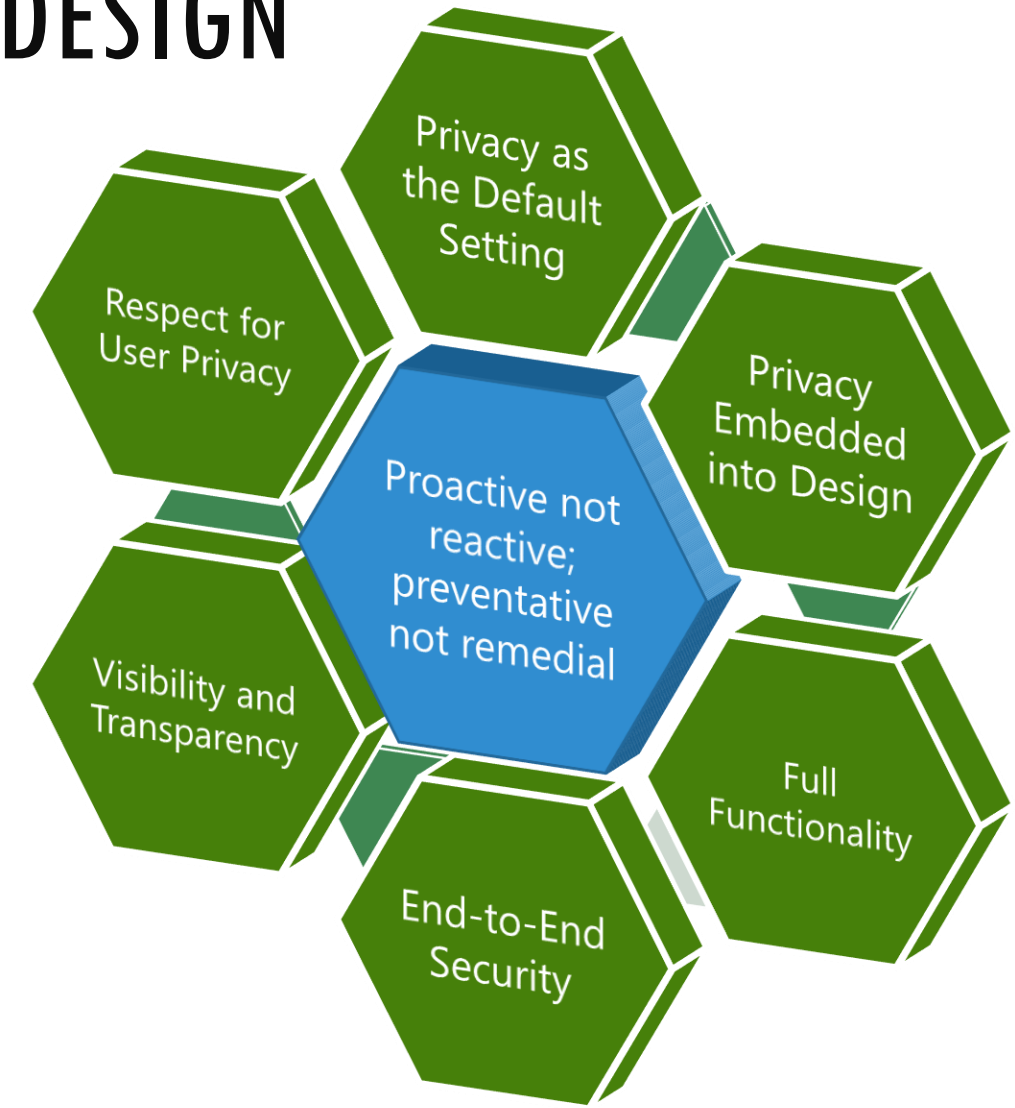
Developed by Dr. Ann Cavoukian in 90' in Canada

"The Privacy by Design framework prevents privacy-invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred; it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after."

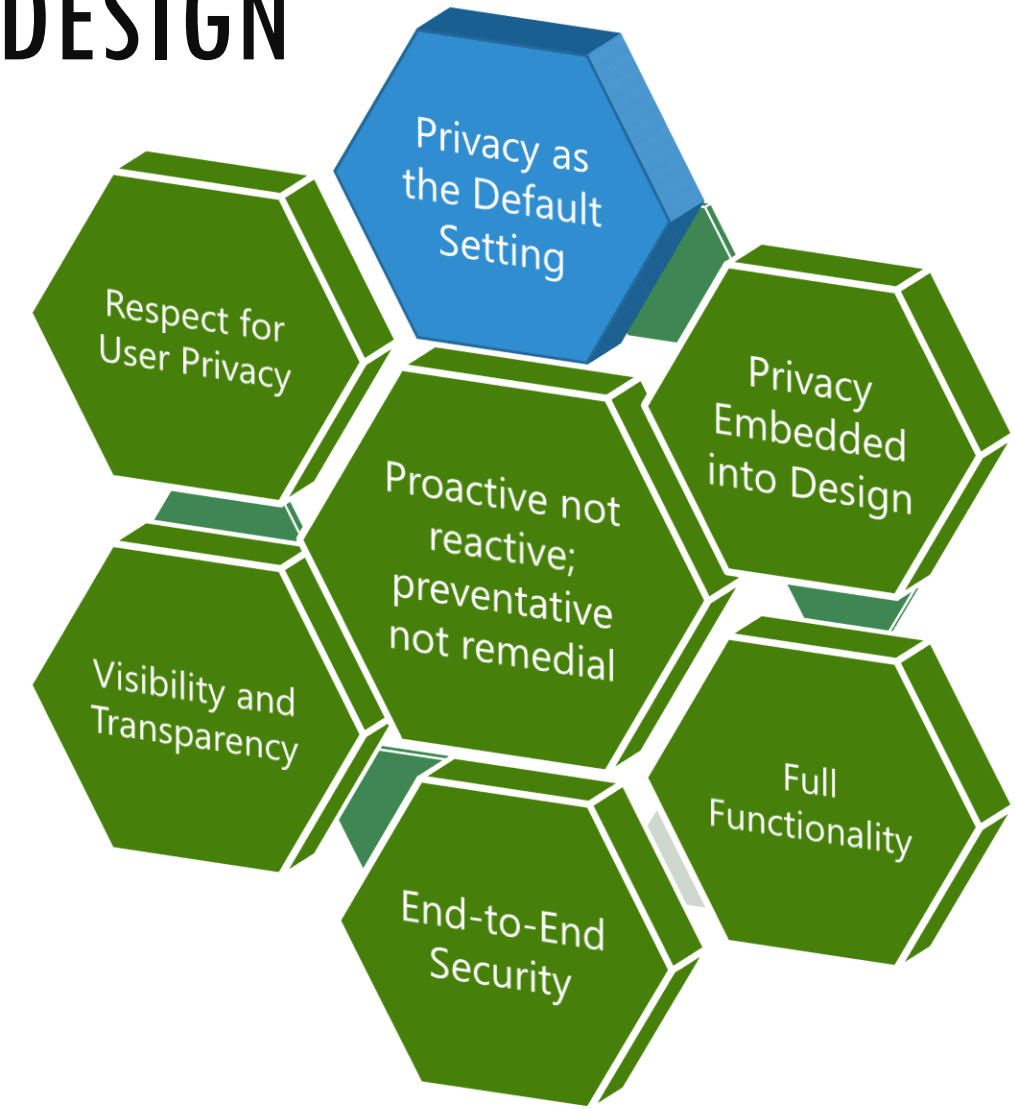
PRIVACY BY DESIGN

1. Proactive not reactive; preventative not remedial
2. Privacy as the Default Setting
3. Privacy embedded into design
4. Full functionality
5. End-to-end security
6. Visibility and transparency
7. Respect for user privacy

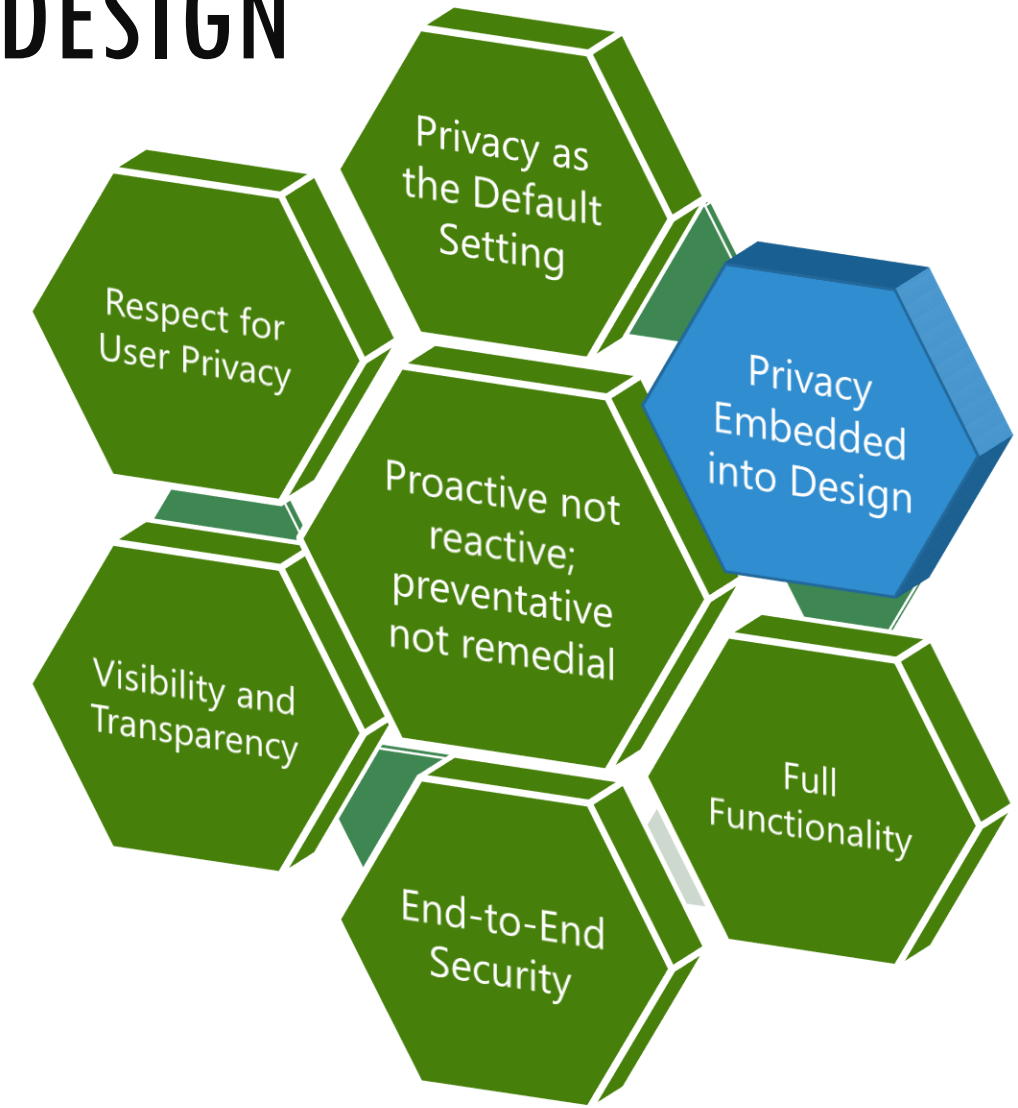
PRIVACY BY DESIGN



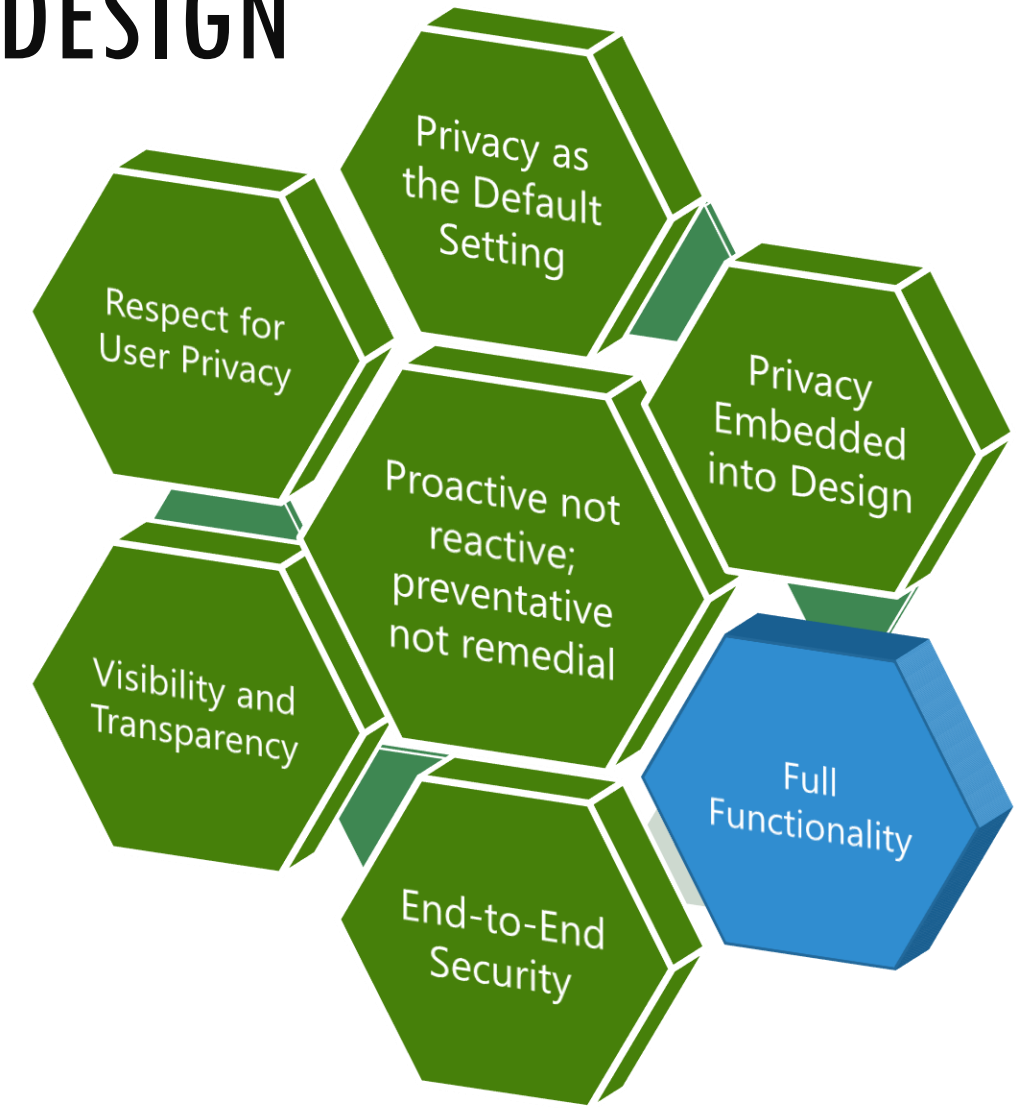
PRIVACY BY DESIGN



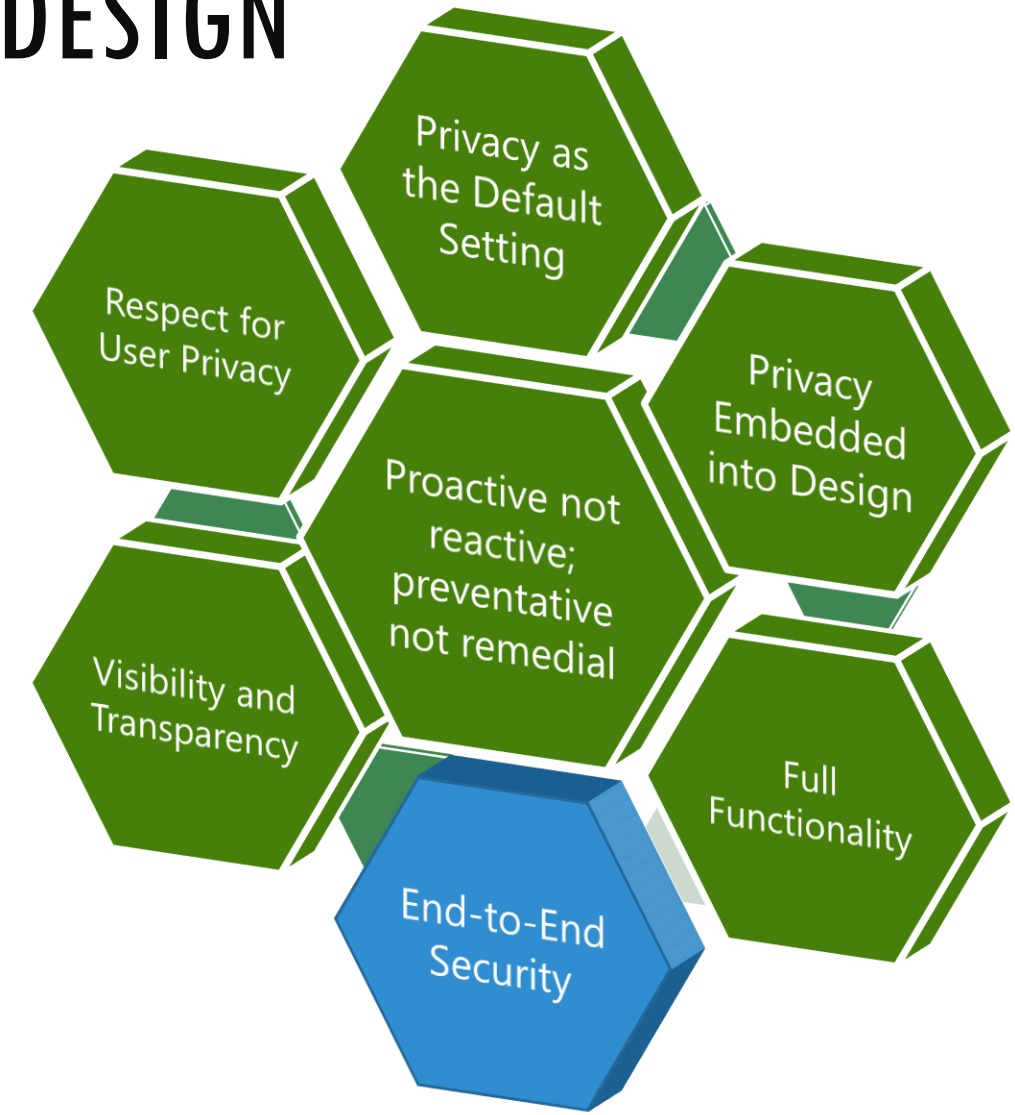
PRIVACY BY DESIGN



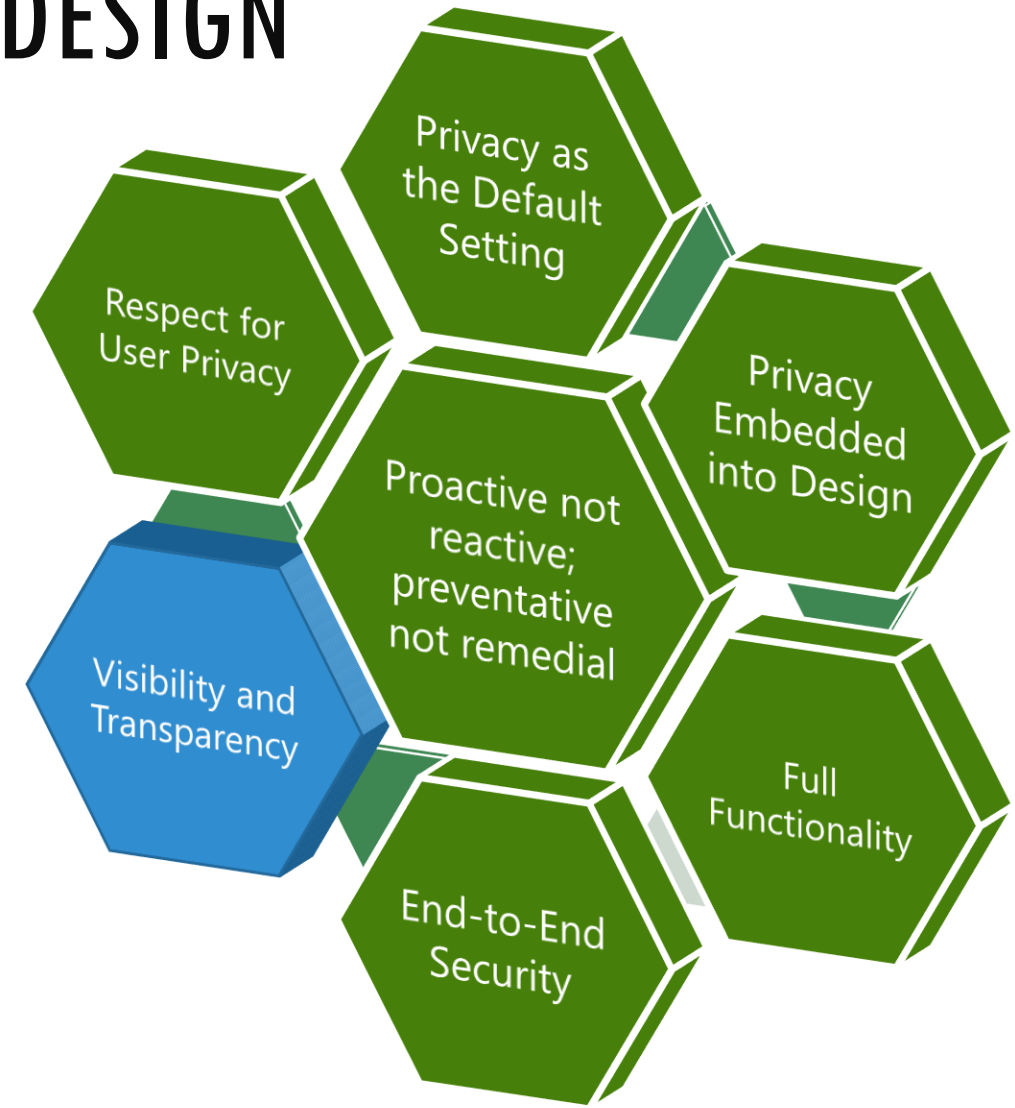
PRIVACY BY DESIGN



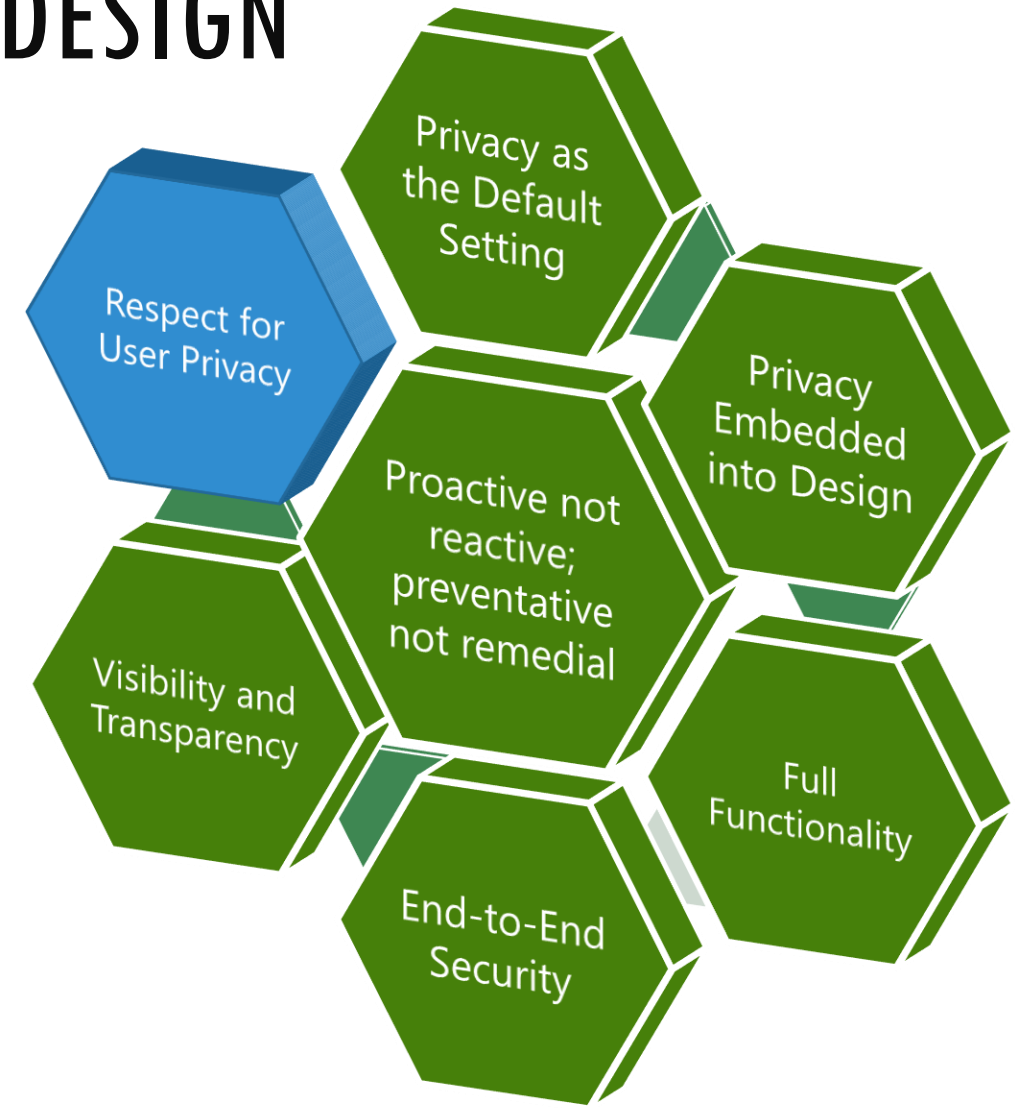
PRIVACY BY DESIGN



PRIVACY BY DESIGN



PRIVACY BY DESIGN



YAGNI

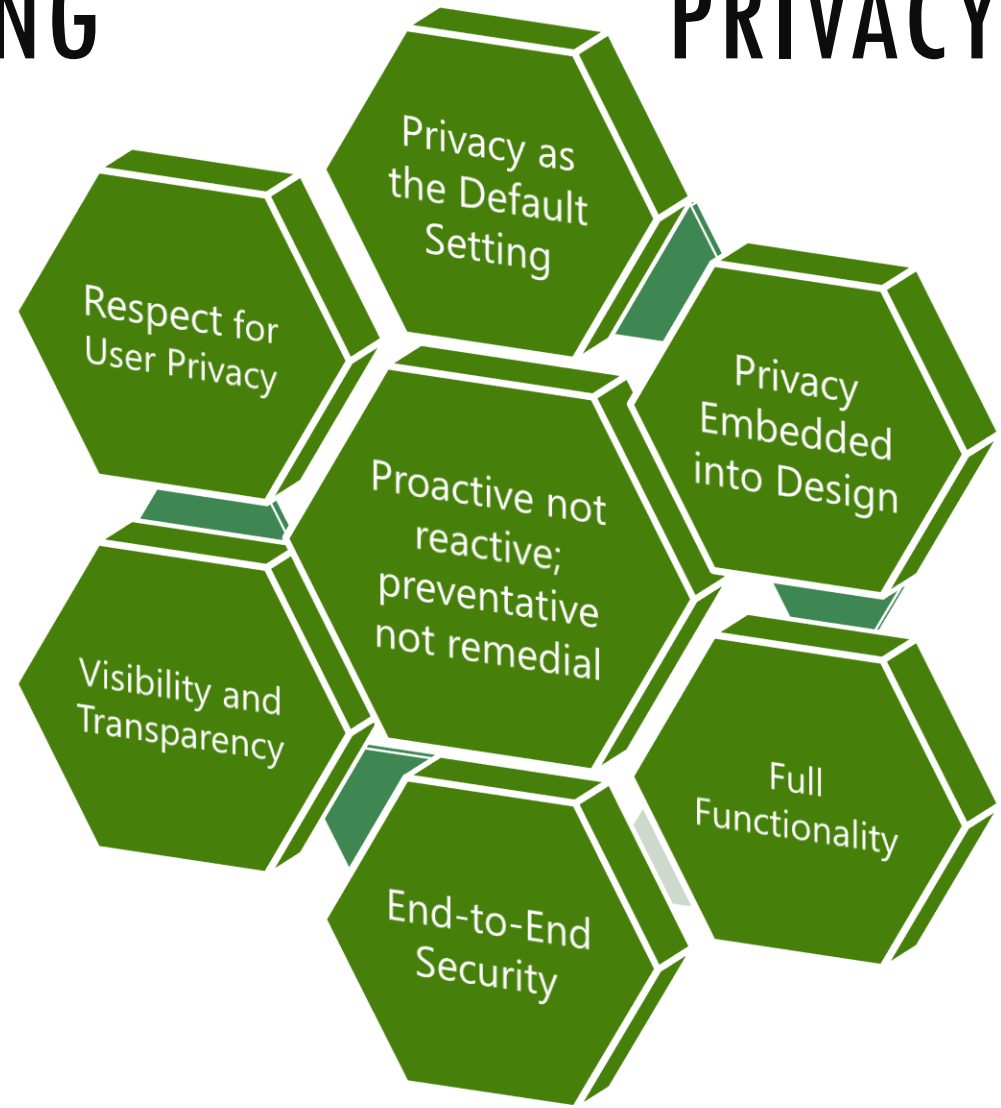
S.O.L.I.D.

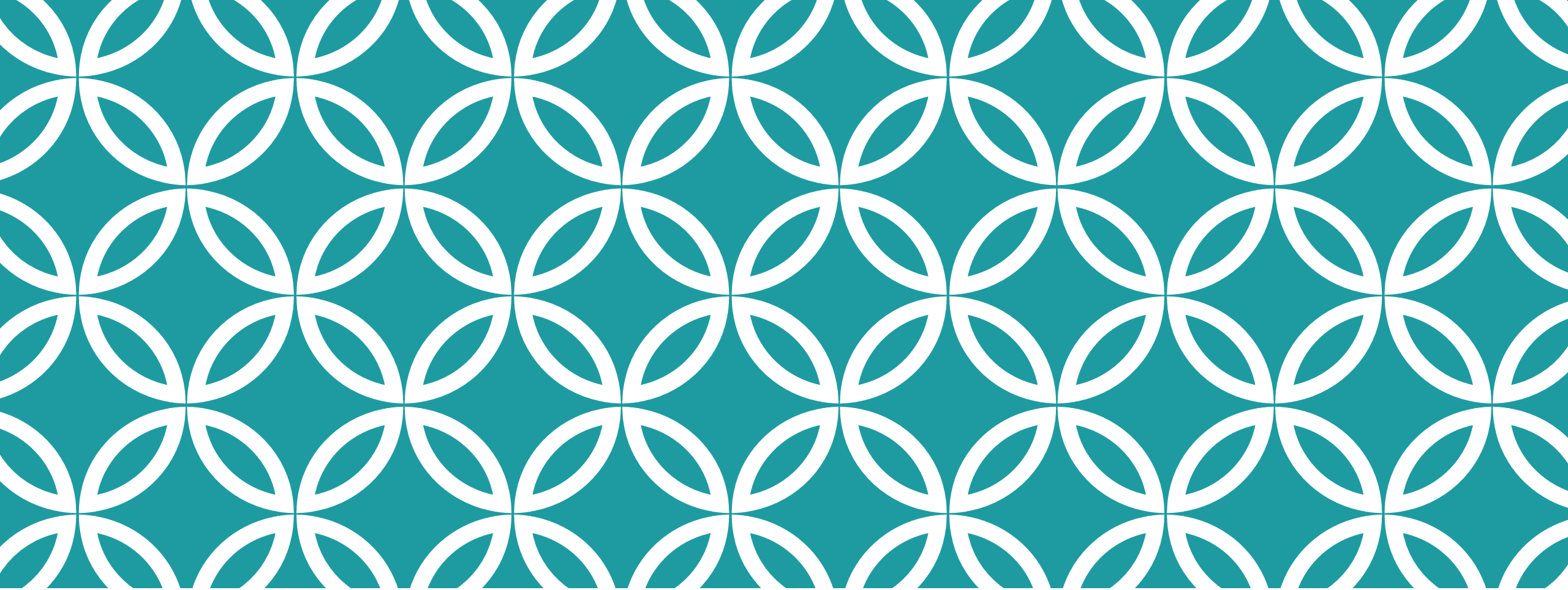
Privacy by Design

DRY

KISS

IMPLEMENTING PRIVACY BY DESIGN



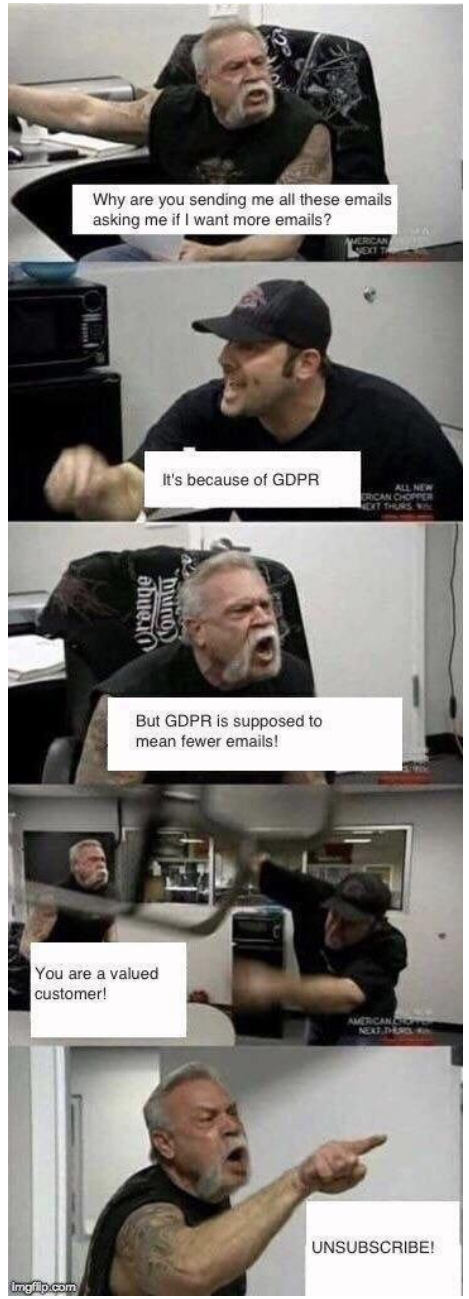


GENERAL DATA PROTECTION REGULATION | GDPR

THE ONLY THINGS CERTAIN IN LIFE ARE DEATH, TAXES AND GDPR…

GDPR

1. Data Protection Directive of 1995 -> GDPR 2018
2. ePrivacy Directive of 2002 -> autumn/winter 2018



DATA SUBJECT

“Refers to natural person that can be identified directly or indirectly through an identifier”


© MARK ANDERSON
WWW.ANDERTOONS.COM
"Before I write my name on the board, I'll need to know how you're planning to use that data."


YOU GET A CONSENT, HE GETS
A CONSENT, SHE GETS A CONSENT
EVERYBODY GETS A CONSENT
imgflip.com

SITECORE - CONSENT

The ConsentInformation facet:

- ConsentRevoked: Gets or sets a value indicating whether the contact has revoked their consent to be contacted by the organization in any form.
- DoNotMarket: Gets or sets a value indicating whether the contact has globally unsubscribed from all marketing lists. This does not include system messages such as order confirmation or “your password is about to expire”.

PERSONAL DATA

“Any information relating to an identified or identifiable natural person or Data Subject”

SENSITIVE PERSONAL DATA

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

PERSONAL DATA DEFINED BY GDPR

GDPR expands the definition of personal data to include:

- Genetic data
- Biometric data (such as facial recognition or fingerprint logins)
- Location data
- Pseudonymized data
- Online identifiers

QUICK CHECK

It is possible for publicly available information to be classified as personal information.

True or False?

a. True

b. False

QUICK CHECK

It is possible for publicly available information to be classified as personal information.

True or False?

a. True

b. False

DATA CONTROLLER

“is the entity that determines the purpose, means, and conditions of processing personal data”

DATA PROCESSOR

“is the entity contracted by the Data Controller to process personal data on their behalf”

GDPR – CORE PRINCIPLES

Fines

- Fines of up to 4% Global Turnover or up to 20 million EUR (which is higher)
- Fines apply to both Processers and Controllers

Breach

- Breach of notification within 72 hours
- Records must be kept of incidents. If It is likely to jeopardize the rights and freedoms of individuals involved

Right to be Forgotten

- Data Subjects have the right to request data controllers to remove personal data under certain circumstances

GDPR – CORE PRINCIPLES CONTINUED

Scope

- Increased territorial scope
- GDPR applies to all processing of personal data of a subject in the EU

Consent

- Explicit and retractable consent
- Must be provided in an easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give

Right to access and portability

- Includes the right to export data between controllers without any hindrance

GDPR – LIGHBULB - QUESTION

Q: How many GDPR consultants does it take to change a lightbulb?

GDPR – LIGHBULB - ANSWER

A: Unfortunately, I can't tell you. The data subjects involved in the experiment did not consent for the information to be released to any 3rd parties.
What I can say is that it was very, very expensive.

GDPR - ACCOUNTABILITY AND GOVERNANCE

- Data Protection Officer
- Data Protection Impact Assessments (DPIAs)
- Breach Notification

GDPR - DATA PROTECTION OFFICER (DPO)

DPO is responsible for ensuring GDPR requirements are met

GDPR - DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

Data Protection Impact Assessments (DPIAs) evaluate the likelihood and severity of potential risk to the Data Subject, and help determine appropriate mitigating measures.

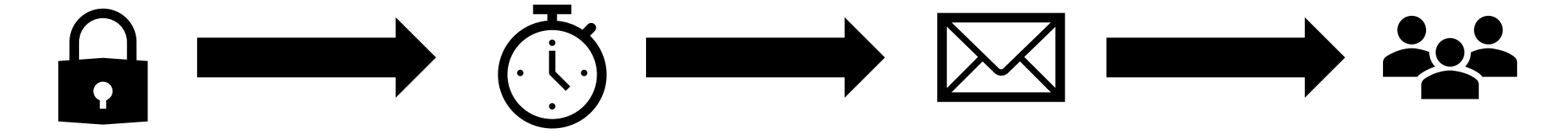
DPIAs are required in the following situations, among others:

- Profiling or automated decision making
- Large-scale use of sensitive personal information
- Large-scale, systematic monitoring
- New data processing technology

GDPR - BREACH

"A personal data breach is a 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."

GDPR - BREACH NOTIFICATION



Data Breach

Within 72 hours of the data breach dictovery

Notify

Data Protection Authority

GDPR – INDIVIDUAL RIGHTS

- Right to Access & Correct Data (Rectification)
- Right to Request a Copy
- Right to Data Portability
- Right to Object or Limit Data Use
- Right to Erasure / Right to be Forgotten

GDPR – RECORD KEEPING

Record Keeping under the GDPR:

- We must maintain a record when processing personal data
- The records of our personal data use must be in writing (including electronic form)
- The records must be made available supervisory authorities and other regulators on request

GDPR – RECORD KEEPING

The record must contain, but is not limited to:

- A description of the categories of individuals
- The categories of personal data
- The purposes of the personal data use
- Legal basis
- Where applicable, disclosure and recipients
- The retention period
- The security measures in place to protect the data

DEMO

GDPR USEFUL LINKS

- GDPR terminology in plain English
- Sitecore 9 Privacy Guide
- Sitecore xConnect - Execute Right to be forgotten
- Sitecore StackExchange GDPR question
- Disable Sitecore Analytics for contact without consent
- GDPR Data Security
- GDPR Support in ASP.NET Core 2.1
- Sitecore Email Cloud to comply with EU GDPR

CONTACT ME

Peter Prochazka

https://tothecore.sk/

https://linkedin.com/in/chorpo/

https://twitter.com/chorpo

https://github.com/chorpo

http://goodreads.com/chorpo

slack

StackExchange

THANK YOU

This page intentionally left blank.