



Privacy by Design with EA

Casimir Artmann
Enterprise Architect

**BCS Enterprise Architecture
Specialist Group**
3rd Annual Conference

Tuesday 2 July 2019
London, UK

#BCS
#BCSEASG
#EASG2019AC

www.bcs.org

Sensitive personal information?



A silver pen with a black and red grip is positioned diagonally in the upper right corner, pointing towards a form. The form is out of focus but contains several checkboxes. The labels for these checkboxes are: Age, E-mail address, Purchase history, Sex, Social security number, Friends & family, DNA, Medical records, Religious belief, Income, Race, Political opinion, Shoe size, Length, Facial recognition, GEO tracking, and Sexual preferences. The background of the form is light-colored with some faint, illegible text.

Age

E-mail address

Purchase history

Sex

Social security number

Friends & family

DNA

Medical records

Religious belief

Income

Race

Political opinion

Shoe size

Length

Facial recognition

GEO tracking

Sexual preferences

Privacy by Design is not a new concept



Ph.D Ann Cavoukian

- Proactive not reactive; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

Facebook, Cambridge Analytica and others

Support The Guardian

Subscribe Search jobs Sign in Search ▾

News

Opinion

Sport

Culture

Lifestyle

More ▾

The Guardian

International edition ▾



The Cambridge Analytica Files

Cambridge Analytica

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower
- Mark Zuckerberg breaks silence on Cambridge Analytica

Carole Cadwalladr and Emma Graham-Harrison

Sat 17 Mar 2018 22.03 GMT

f t e 197,689 484

🕒 This article is over 7 months old



▲ Cambridge Analytica whistleblower: 'We spent \$1m harvesting millions of Facebook profiles' - video

Advertisement

Ad closed by Google

Report this ad

Why this ad? ▶

GDPR and privacy regulations



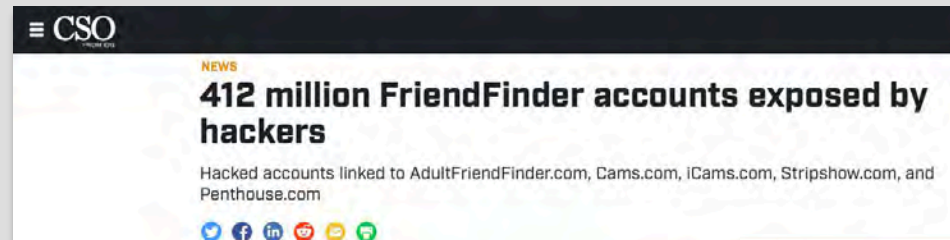
R **Is consent good enough?**

Opt-out



Opt-In

Security breaches are more common



NEWS
412 million FriendFinder accounts exposed by hackers
Hacked accounts linked to AdultFriendFinder.com, Cams.com, iCams.com, Stripshow.com, and Penthouse.com



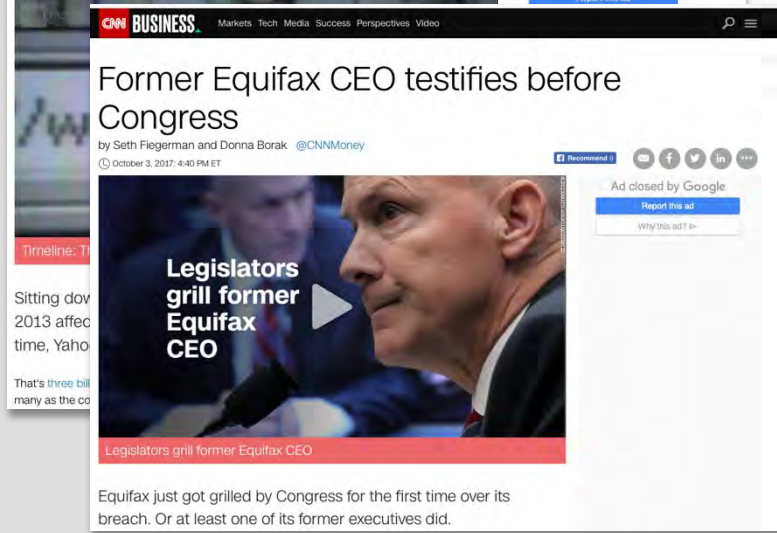
CNN BUSINESS
Markets Tech Media Success Perspectives Video
Every single Yahoo account was hacked - 3 billion in all
by Selena Larson @selenalarson
October 4, 2017, 6:26 AM ET



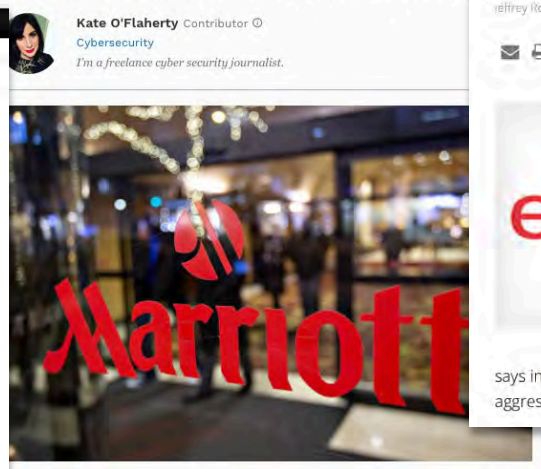
RISE ABOVE THE NOISE.
Extra-ION Reveals network traffic analysis
Chaires Innovation Leadership Money Consumer
Marriott CEO Reveals New Details About Mega Breach



Topics - News - Training - Resources - Events - Jobs -
TRENDING: View ISM's R5AC 2019 Coverage | 160+ Video Interviews Featuring Top Industry Thought Leaders
eBay Breach: 145 Million Users Notified
Users Urged to Change Passwords After Database Compromise
jeffrey Roman (@gen_sec) • May 21, 2014
eBay is urging its 145 million customers to change their passwords following a cyber-attack that compromised encrypted passwords and other personal information.
See Also: Webinar | The Future of Adaptive Authentication in Financial Services
The attack, which occurred between late February and early March, originated after a small number of employee log-in credentials were compromised, which enabled cyber-attackers to gain access to eBay's corporate network, eBay says in an **FAQ**. "We are working with law enforcement and leading security experts to aggressively investigate the matter," the company says.



CNN BUSINESS
Markets Tech Media Success Perspectives Video
Former Equifax CEO testifies before Congress
by Seth Flegeman and Donna Borak @CNNMoney
October 3, 2017, 4:40 PM ET
Legislators grill former Equifax CEO
Equifax just got grilled by Congress for the first time over its breach. Or at least one of its former executives did.



Kate O'Flaherty Contributor
Cybersecurity
I'm a freelance cyber security journalist.

Privacy by design and privacy by default

Privacy by design means that the privacy protection rules are taken into account already when IT systems and procedures are designed.

It is a way to ensure that the General Data Protection Regulation's requirements are complied with and that the data subjects' rights are protected.



Design business for privacy

Process design requirements

- **Inform** the individual how his/her data is used and for what purpose
- Give **Control** over the personal data for the individual
- **Enforce** documentation how the personal data is protected
- **Demonstrate** how to control and follow up



Inform

Example – Privacy policy

- What information do we have?
- How do we use the information?
- Who do we provide information for?
- Sharing information on social media
- Your privacy rights
- Child protection



Control

Example – Customer self service in Norway



Source: Aller Media

Dine abonnement

Velkommen! Her kan du enkelt administrere ditt eget abonnement og bl.a.:

- Endre leveringsadresse
- Legge inn midlertidig ferieadresse
- Legge inn feriestopp for en gitt periode
- Få gode tilbud på våre andre publikasjoner
- Oppdatere kontaktinformasjon
- Endre passord
- Kjøpe gaveabonnement
- Verve nye abonnenter

For å logge deg inn, begynn med å taste inn *enten*

- din e-postadresse
- *eller* ditt telefonnummer
- *eller* ditt kundenummer her:

Gå videre >>

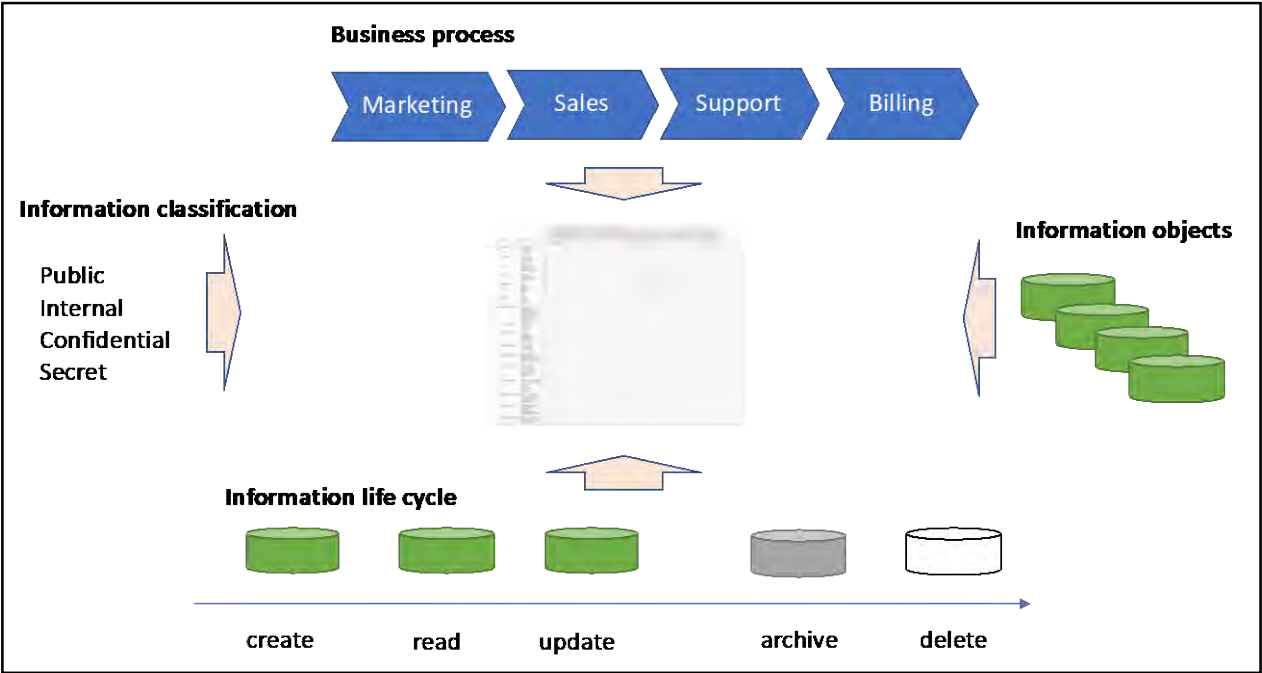
Ofte stilte spørsmål

[+ Hvor finner jeg kundenummeret mitt?](#)

Enforce

Example – Architecture documentation

- Involved parties
- Business Processes
- Information Models
- Information Classification
- Information Lifecycle
- Used applications
- Used infrastructure
- Location of infrastructure

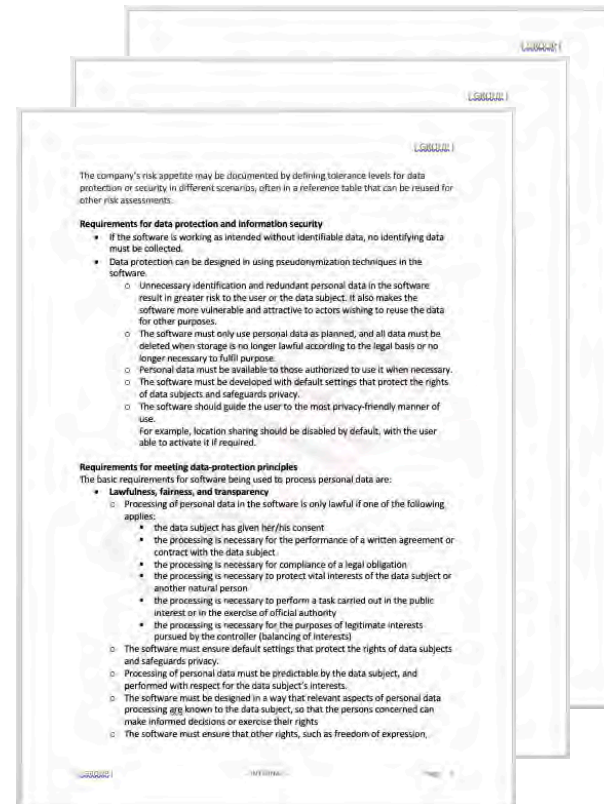


Architecture view: Business process and information modelling

Demonstrate

Example – Checklists for reviews

- Mandatory requirements for management
- Training
- Requirements
- Design
- Coding
- Testing
- Maintenance



Design IT-systems for privacy

A person is shown from the side, holding a smartphone and looking at the screen. The background is dark with many out-of-focus, warm-colored lights (bokeh), suggesting an urban or indoor setting at night. The person is wearing a dark jacket. The overall mood is focused and modern.

Data design requirements

- **Minimize and limit** amount of collected personal data
- **Hide and protect** personal data and their relations
- **Separate** different types of personal data for different purposes
- **Aggregate** personal data and avoid detailed personal data
- **Data protection by default**

Minimize and limit

Example – Call Data Record

A Call Data Record contains data fields describing a particular instance of a telecommunications transaction, but does not include the contents of this transaction.

- the telephone number of the subscriber coming from the call (calling party, A-party)
- the phone number that receives the call (called party, B-party)
- the start time of the call (date and time)
- call duration

Field	Category	Tag	Data Type
pGWRecord	M	0xBF4F	SET
recordType	M	0x80	INTEGER
servedIMSI	C	0x83	TBCD-STRING (SIZE (3..8))
pGWAddress	M	0xA4	CHOICE
chargingID	M	0x85	INTEGER (0..4294967295)

Field	2G	3G	TAG	TYPE
recordType	M	M	0x80	ENUMERATED (SIZE(2))
servedIMSI	O	O	0x81	TBCD-STRING(3..8)
servedIMEI	O	O	0x82	TBCD-STRING(8)
servedMSISDN	O	O	0x83	ADDRESS(2..9)
callingNumber	C	C	0x84	ADDRESS (2..17)
calledNumber	M	M	0x85	ADDRESS (2..17)
translatedNumber	O	O	0x86	ADDRESS (2..17)
connectedNumber	O	O	0x87	ADDRESS (2..17)
roamingNumber	O	O	0x88	ADDRESS (2..17)
recordingEntity	M	M	0x89	ADDRESS(2..9)
mscIncomingROUTE	O	O	0xAA	CHOICE (SIZE (1..9))
mscOutgoingROUTE	O	O	0xAB	CHOICE (SIZE(2))
location	M	M	0xAC	SEQUENCE

Hide and protect

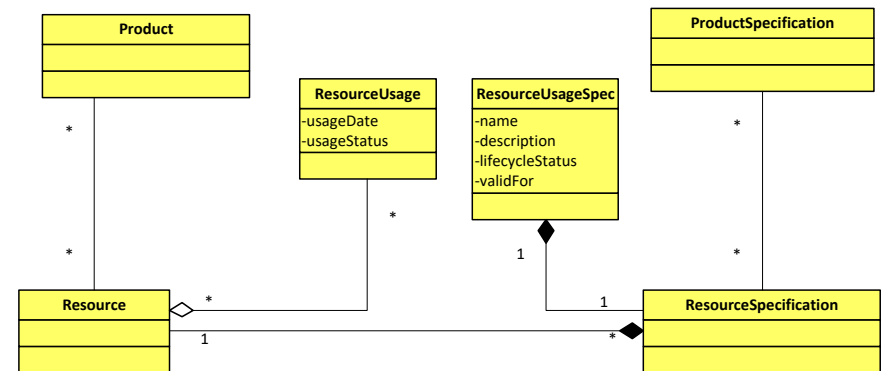
Example – Call Data Record

The availability of call history is limited, as it may contain confidential or secret information

Within EU

- Only handed out by court order
- Only stored for a limited time

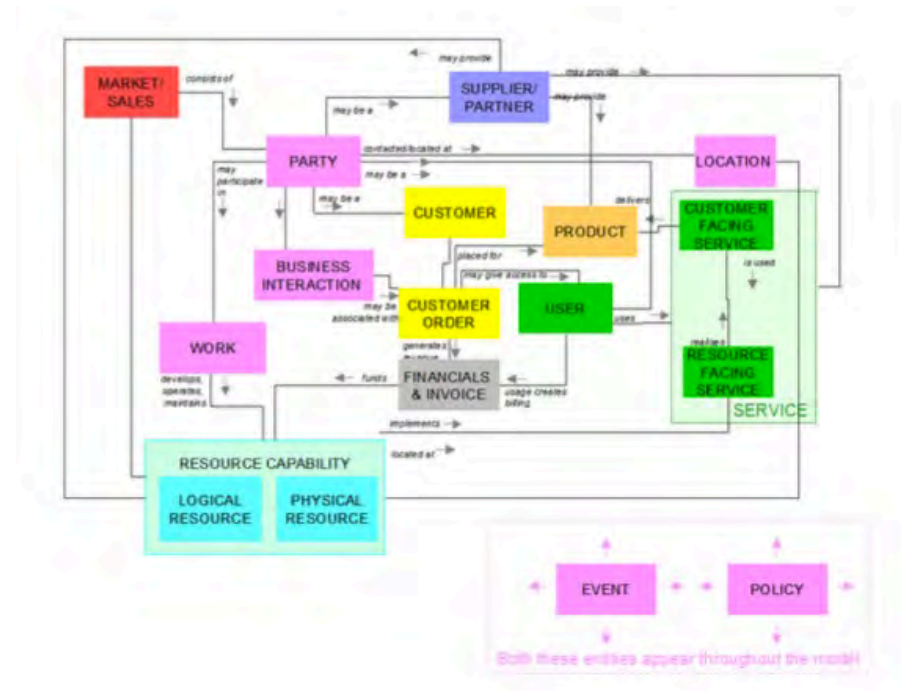
We need security related services as access control, logging, data retention and encryption of data to fulfill business requirements



Separate

Example – Call Data Record

A call data entry does not contain names or social security numbers, but may be associated with a single subscription (Product)



Aggregate

Example – Call Data Record

The data from the call log gathered for billing purposes can also be used for other purposes by the operator and its partners

- Need to aggregate or anonymise personal data for other purposes



Data protection by default

We need to design new systems so that we only handle the data needed for the purpose, and not more

5G



State sponsored hackers



Zero trust security



Privacy governance



Legal compliance



Damage limitation



Increased brand value

Brand Value

Credits

Writer

Casimir Artmann

Stock footage

Adobe

Illustrations

TM Forum

Newspapers

The Guardian

CNN

CSO

Forbes

Bank Info Security

Behind the scenes

	Business aspect area	Information aspect area	Application aspect area	Infrastructure aspect area	Governance	Security
Contextual layer	Ann and her seven principles Facebook, Cambridge Analytica and others Privacy by design and privacy by default State sponsored hackers Damage limitation Value of privacy for individuals Value of privacy for brand					
Conceptual layer	GDPR and privacy regulations Is consent good enough Design business for privacy	GDPR and privacy regulations Sensitive personal information	GDPR and privacy regulations Design IT-systems for privacy	GDPR and privacy regulations	GDPR and privacy regulations Privacy governance	GDPR and privacy regulations Zero trust security
Logical layer	Design business for privacy		Design IT-systems for privacy		Privacy governance	Zero trust security
Physical layer						