Putting Privacy by Design Principles into Practice

Adil Akkuş

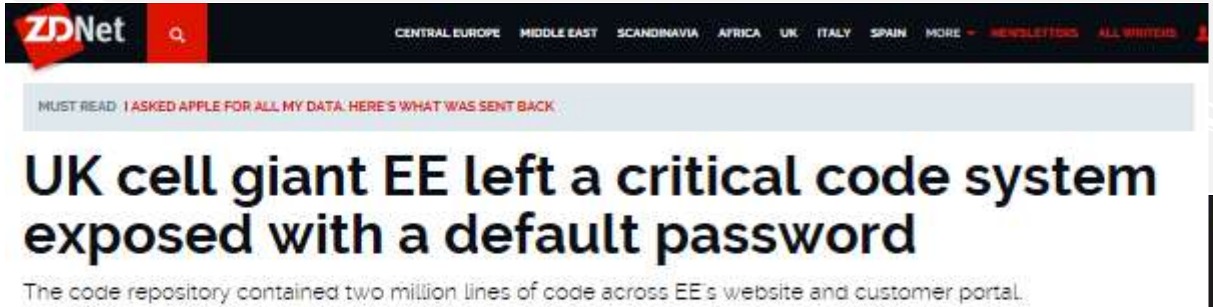
90% world’s data is estimated to be collected over the last 2 years

Data is the new currency

- Uber, the world’s largest taxi company, owns no vehicles
- Facebook, the world’s most popular media owner, creates no content
- Alibaba & Amazon, world’s largest retailers, have no inventory
- Airbnb, the world’s largest accommodation provider, owns no real estate

Privacy threats to ourselves and our customers very real

- **EE** – according to reports 2 million lines of code was exposed (with AWS keys, API keys and more)
- **Facebook / Cambridge Analytica** – 87 million people's data was mined
- **Uber** – 20 million people's data was exposed
- **Equifax** – 143 million consumers' sensitive personal information was exposed
- **Yahoo** – over 500 million accounts were hacked
- **MyFitnessPal** – Hackers stole data of more than 150 million users



MUST READ I ASKED APPLE FOR ALL MY DATA. HERE'S WHAT WAS SENT BACK

UK cell giant EE left a critical code system exposed with a default password

The code repository contained two million lines of code across EE's website and customer portal.

NOTICE OF DATA BREACH

Regulators ratchet up pressure on Facebook over user data leak

US | Nov 21, 2017

2016 Data Security Incident

— Written by Dara Khosrowshahi, CEO

- Some of these breaches remained undetected, unreported or unknown for various reasons.
- A good proportion of these incidents could have been prevented or handled in a much less costly and much less distressing way by using the Privacy by Design framework.

$150

Estimated cost for each lost or stolen ***record*** containing sensitive and confidential data

2017 Ponemon Cost of Data Breach Study (https://www.ibm.com/security/data-breach)

- With the undeniable influence of GDPR, regulators and the public expect the “privacy by design” principles to prevent such high profile cases and to increase public’s confidence in the organisations with their data.
- Until recently the data protection teams had to fight hard to convince the product, service and the technology teams to pay attention to privacy concerns, GDPR’s emphasis on “privacy by design” will transform our ways of working and thinking.
- Long-term success of privacy by design adoption require a **culture shift**

Principle 1: Proactive not Reactive; Preventative not Remedial

Anticipating and preventing privacy invasive events before they happen. Do not wait for privacy risks to materialize – the aim is to prevent the breaches from occurring.

	Actions
1	Secure senior **leadership commitment**
2	Ensure that **tangible actions**, not just policies, reflect a commitment to privacy
3	Use **Privacy Impact Assessments** to assess privacy & security risks and to correct any negative impacts, well before they occur
4	Share and demonstrate privacy practices with diverse user communities and stakeholders. Consider establishing a **privacy network**.

Principle 2: Privacy as the ***Default Setting***

- *Delivering the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice.*
- *No action should be required on the part of the individual user to protect their privacy – it should be built into the system, automatically – by default.*

	Actions
1	Adopt as **narrow and specific a purpose(s)** for data collection as possible
2	**Minimize data collection** at the outset to only what is strictly necessary
3	Limit the use of personal information to the **specific purposes** for which it was collected
4	Create **barriers to data linkages** with personal data

Principle 3: Privacy ***Embedded*** into Design

- *Privacy measures are not bolted on as add-ons, after the fact.*
- *Privacy should be an essential component of the core functionality being delivered.*

	Actions
1	Make a **Privacy Risk Assessment** an integral part of the design stage of any initiative
2	Consider privacy in system development lifecycles and organizational engineering processes
3	Adopt a set of fundamental principles for **regulate identity architecture**
4	Make your **data flows transparent**
5	Provide **granular controls** over data flows

Principle 4: Full Functionality – ***Positive-Sum***, not Zero-Sum

- *Accommodating legitimate interests and objectives in a positive-sum, 'win-win' manner, not through a zero-sum (win/lose) approach, where unnecessary trade-offs to privacy are made.*
- *Avoiding the pretense of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.*

	Actions
1	Acknowledge that multiple, legitimate business interests must **coexist**
2	**Understand, engage and partner** with stakeholders
3	Pursue innovative solutions and options to achieve multiple functionalities

Principle 5: End-to-End Security – ***Full Lifecycle Protection***

- *Security is the key to privacy. These actions ensure cradle-to-grave, lifecycle management of information, end-to-end, so that at the conclusion of the process, all data is securely destroyed, in a timely fashion.*

	Actions
1	Employ **encryption by default** to mitigate the security concerns
2	Deploy encryption correctly and carefully integrate it into devices and workflows in an automatic and **seamless manner**
3	Ensure the secure **destruction** and disposal of personal information at the end of its lifecycle

Check Out ENISA (EU Agency for Network and Information Security)
https://www.enisa.europa.eu/

Principle 6: ***Visibility*** and ***Transparency*** – Keep it ***Open***

- *Stakeholders must be assured that whatever the business practice or technology involved, it is, in fact, transparent to the user, and operating according to the stated promises and objectives, subject to independent verification.*
- *Remember, trust but verify.*

	Actions
1	Consider a **layered approach** to your privacy notices
2	Go beyond the legal jargon, write the privacy notices in “plain language”
3	Where possible, **make the privacy notices engaging**

Principle 7: ***Respect*** for User Privacy – Keep it ***User-Centric***

- *This method requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.*
- *Keep it user-centric.*

	Actions
1	Offer **strong privacy defaults**
2	Provide **appropriate notices**
3	Consider user-friendly options: a. Provide users with access to data about themselves b. Provide access to the information management practices of the organization
4	**Allow users to consider to explicitly consider the context of their data** and how they can adjust the associated data flows

“Good enough” isn’t any more!

- Adopting Privacy by Design will create new procedures to follow. Adoption may feel onerous but this is **necessary in our rapidly changing world**
- Embracing the Privacy by Design principles will help reduce your privacy risks.
- Use GDPR as an opportunity to improve the user experience, user trust and ultimately your business reputation