RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: PRV-W02

Lesson Learned:
What I Have Experienced While Implementing GDPR

Michael Mrak

Casinos Austria AG
@michael_mrak

RSAConference2019

Are you affected by the GDPR?


That's how I looked at it ...


after the GDPR was published.

The starting situation was decisive
… for a “relatively” simple implementation

We have always dealt well with personal data

- A well-established privacy system has existed since 2009
- We have had data protection certified since 2010
- A directory of processing activities has existed since 2010
  - We call it directory of data protection relevant objects and use the same information for the list of assets also required for information security purposes
- Fortunately, there is a very high level of awareness regarding the handling of personal data in my company

RSAConference2019

A giant project briefly explained

From spring to autumn 2017

- Update of the existing data protection management system
- Update of the the existing documentation of all data protection relevant objects (list of processing activities)
- Identification and evaluation of all data collections that need to undergo an extended risk analysis
  - Privacy Impact Assessment
- Risk-based implementation of the necessary measures to ensure data protection compliance in the affected systems

From autumn 2017 until May 2018
… uh, actually until today

- Review of all contracts with service providers (data processors)
- Update of consent statements
- Adding data breach notification crisis processes to emergency management (Data Breach Notification Duty)
- Training of all employees and internal privacy coordinators
- Roadshow and training through all our casinos & rollout of a compulsory e-learning for all employees
- A lot of documentation work

RSAConference2019

The biggest challenges

Technical limits and social aspects

- Some requirements can simply not be implemented
  - A guide for deletion of personal data is ready BUT
    - The technical implementation of the concept for data deletion will take years
    - The documentation of all external data protection requests must be ensured
- Although the implementation was set up as a cross-company project, there were often other priorities for the individual business units
- The internal communication effort was enormous

RSAConference2019

End of the project ≠ End of work

The journey to full GDPR compliance has just begun

- Significantly more customer inquiries about data protection
- The difference between privacy requests and responsible gaming queries is often not obvious at first glance
- Data protection is now an integral part of all projects in which personal data is used
  - This is already clearly defined in projects today
  - But what about small workgroups that are not subject to the project guidelines?
  - How to keep awareness high at management level in the future?

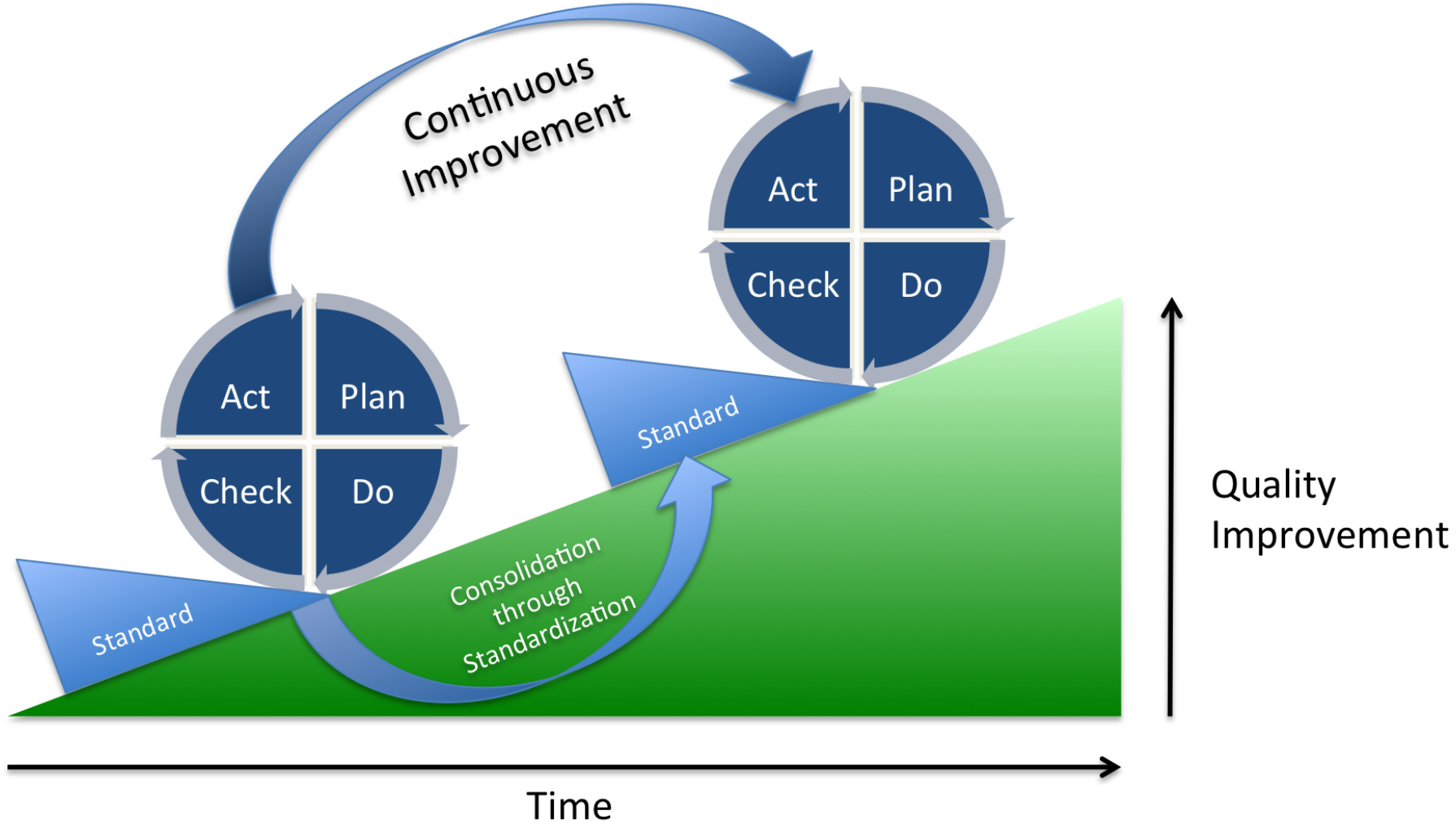
RSAConference2019

Which of you has a system in which all personal data is automatically deleted upon request or after the expiry of the permitted storage period?

The journey to full GDPR compliance has just begun

- The implementation for the automatic data deletion will cost a lot of money and nerves
- All measures taken must be periodically reviewed (PDCA management cycle)
- Legal developments will lead to changes

Improving the GDPR compliance



RSAConference2019

Some final takeaways!

Important takeaways

- Consider data protection as an elementary pillar of compliance
- Search internal allies
- Never underestimate the communication effort
- Search for synergies with existing management systems
- The conversion of the GDPR leads to more quality

The GDPR could be the global „gold standard“ for data protection

Microsoft is among the global technology firms that will have to comply with the laws in Europe and -- pointing out how it appreciates "the strong leadership by the European Union on these important issues" -- the company says that it will also roll out the benefits of the privacy legislation on a global basis. It will be known as Data Subject Rights

Julie Bril, Microsoft's corporate vice president and deputy general counsel,

“We’re already seeing a number of countries falling in line with Europe” — *Eduardo Ustaran, co-director of the global Privacy and Cybersecurity practice of Hogan Lovells*

“Any country that’s not working toward these standards is left out in the cold,” said John Giles, managing attorney at Michalsons, a law firm in South Africa. “GDPR has long tentacles.”

E-Mail: michael.mrak@casinos.at
Phone: +43 664 5032331
governance.cal.at
www.linkedin.com/in/mmrak
@michael_mrak