schönherr

to the point technology & digitalisation

Preface

Cyber risk and GDPR

This past year has forced us to adapt in various ways. "Normal" work life quickly moved from dropping the kids off at school on the way to the office to working from home while keeping an eye on the kids' distance learning. But the pandemic also changed the work life of criminals. While the number of burglaries has dropped, cybercrimes are at a new all-time high. Home office networks have formed new gateways for cybercriminals. From a company's perspective, cybercrimes are a multi-layered threat: the company's data and business secrets are exposed, its reputation is at risk, GDPR compliance becomes even harder to ensure, and considerable fines more difficult to avoid. This might be why the European Data Protection Board released new complementary Guidelines on Data Breach Notifications ("Guidelines" to be found here) earlier this year. These new Guidelines provide examples of best practices to prevent data breaches in the first place and explain how to assess the GDPR-related consequences (i.e. notification of supervisory authority YES/NO, notification of data subjects YES/NO). Clearly, the Guidelines are based on the EU-wide experience the national supervisory authorities have collected over the last (almost) three years. The Guidelines further show – once more – the European Data Protection Board's effort to seek "technical solutions", like high standards of data encryption at rest, electronic back-up systems, etc. The draft Guidelines were open for public consultation until March 2nd.

EDPB Examples re Data Breach Notification

Risks identified / samples provided by the EDPB:

- ransomware
- data exfiltration attacks
- internal human risk source
- lost or stolen devices and paper documents
- mispostal (accidental and on purpose)
- other cases – social engineering

For each of the above-mentioned categories of risks the EDPB analysed:

- prior measures: what controllers should do to prevent breaches in the first place
- risk assessment: how a controller will evaluate the risk
- mitigation steps: mitigating measures a controller should take if a breach occurs
- obligations: whom to notify if a breach occurs and how to document a breach internally

Veronika Wolfbauer
Counsel, Austria
v.wolfbauer@schoenherr.eu
T: +43 1 534 37 50791

To the Point:

- **New facial recognition guidelines**
  On 28 January 2021, the Council of Europe published a new set of guidelines on the use of facial recognition technologies ("**Guidelines**"). The Guidelines, addressed especially to governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies, indicate that AI technologies using facial recognition are an extremely sensitive matter and may pose a real threat to the rights of data subjects, including their right to privacy. In general, it is the legislators' responsibility to ensure the accountability of facial recognition developers and providers, including through the creation of appropriate certification mechanisms. The Guidelines also emphasise that any measures taken should evolve over time and be proportionate to the sensitivity of the data, as the privacy of data subjects is of the essence. Those to whom the Guidelines are addressed should now work hard to achieve a perfect balance between the proposed restrictions and continuing technological development. Read the full article here.

  Daria Rutecka

- **The Digital Assets Act – New Tech Regulation in Serbia**
  The Serbian Parliament enacted the new Digital Assets Act ("**DAA**"), which will come into force on 29 June 2021. The main points of the new framework are outlined below, and the topic is discussed in more detail in our latest blog article here:

  - The DAA regulates all digital assets regardless of the technology on which those digital assets are based.
  - The DAA recognises two types of digital assets: virtual currencies and digital tokens.
  - The DAA recognises the concept of digital assets mining, but this area is excluded from the scope of the DAA.
  - The government authority with competence over virtual currencies is the National Bank of Serbia ("**NBS**"), while the authority with competence over digital tokens is the Serbian Securities Commission ("**SEC**").
  - Digital assets can be issued with or without a "white paper".
  - Secondary and OTC trading are allowed with or without an intermediary, and the use of smart contracts is explicitly allowed for secondary trading.
  - Digital assets services providers must be incorporated in Serbia and hold the appropriate NBS/SEC licences.
  - A pledge may be established over digital assets, but it must be registered with a service provider specifically licensed to operate a digital asset pledge register.
  - Parties may enter into a fiduciary agreement for securing receivables or for other purposes.
  - Fines and criminal liability: the maximum penalty for a breach of the DAA is RSD 5,000,000 (approx. EUR 43,000) or up to 10 % of annual turnover for the preceding financial year, whichever is higher. Individuals engaged in insider dealing or market manipulation may also be criminally liable (with a prison term of five to eight years and a fine).

  Mina Mihaljčić

- **When will your order be delivered by drone?**
  While it will probably be a long time before someone flies to your door in an Iron Man suit to deliver your Amazon package, having a package delivered by drone is closer than we think.
  Used mainly for recreational purposes as well as in media and entertainment, drones are slowly but surely gaining ground in commerce, too. How close we are to having our packages delivered with the help of drones depends largely on how soon certain legislative gaps are filled.
  Companies in the trade and logistics sectors are intrigued by the potential benefits drone technology could bring to delivery services. In fact, the authorities have begun to create a regulatory framework for the use of drones in the European Union, following the example of the United States, where drones are already being flown at an early stage for various commercial delivery activities.
  In 2020, common rules for the use of drones in the EU area, published in 2019 by the European Union Aviation Safety Agency, entered into force. They create universal guidelines for what drone operators in the EU may or may not do. Also, with effect from 31 December 2020, EU Regulation 2019/947 on the rules and procedures for the operation of unmanned aircraft systems ("**UAS**") applies in EU Member States.
  For a more detailed overview on the potential of drone deliveries and on legislation applicable for using and operating drones, please see our blog.
  Vlad Săndulescu
  Visit Eva Bajáková's blog to learn more!

- **MARQUES Copyright Directive tracker**
  Digital technologies have fundamentally transformed the way creative content is produced, distributed and accessed. Will the EU Copyright Directive bring copyright rules up-to-date to meet the comprehensive requirements of the "digital era"?

  Check out the MARQUES Copyright Directive tracker that summarises key information on the legislative process (such as the status, date and other information) on the implementation status of the EU Copyright Directive (2019/790) in the EU Member States, including various Schoenherr contributions for Austria, Bulgaria, Croatia, the Czech Republic, Hungary, Poland, Romania, Slovakia and Slovenia.
  Christian Schumacher & Anna Katharina Tipotsch

- **The number of whistleblower tips has increased sharply. More than half concern investment fraud, especially with crypto assets**
  In 2020, 278 tips were submitted via the whistleblower platform on the Austrian Financial Market Authorities (FMA) website. This is a new record high since the introduction of the system in 2014 and an increase of 57 % in the past five years alone. This information channel is becoming increasingly popular because it technically guarantees whistleblowers absolute anonymity, which creates trust and security.
  With the current crypto boom there are also more and more people who want to make money from it in a fraudulent way. Two-thirds of the indications of investment fraud today already concern offers in connection with crypto assets and virtual currencies, with sales taking place via dubious or criminal online trading platforms, often advertised via social media like Facebook, WhatsApp, TikTok or Telegram. In 2020 alone, whistleblower tips led to seven investor warnings, 42 reports to the public prosecutor's office, and many regulatory proceedings by the FMA as well as penalty findings. The full press release can be read in German here.
  Dominik Tyrybon

- **Epic Games (and others) vs Apple – rounds 2, 3 and 4**
  As we reported earlier, Epic Games launched antitrust litigation against Apple (and Google) in California. The case concerns Apple's removal of the hugely popular battle royale game Fortnite from the App Store after Epic introduced its own direct in-app payment functionality into the version of Fortnite available on iOS, in contravention of the terms of Apple's Developer Agreement. Epic filed an additional claim against Apple in Australia in November 2020 (round 2), and then just before Christmas, Epic filed a lawsuit against Apple and Google in the UK before the Competition Appeal Tribunal ("**CAT**"; round 3). A summary of the UK claim can be found here and is grounded basically on the same reasons as the California claim: Apple is violating competition rules by i) reserving to itself the sole channel for the distribution of apps to and/or the payment processing mechanism for purchases of in-app content for and by consumers who use iPhones and iPads, ii) using its dominant position to charge unfair prices for the distribution of apps via the App Store and/or use of the Apple in-app payment processor, and iii) its response to Epic's introduction of price competition for purchases of in-app content in Fortnite.
  However, the key defendants, Apple Inc, Alphabet Inc and Google LLC are all domiciled outside the UK, which is why the competent court in the UK ruled at the end of February that Epic Games is cleared to sue multiple Google entities as well as Apple (UK) Limited in the Competition Appeal Tribunal (sitting in England and Wales), and cannot sue Apple Inc. (the Cupertino-based corporate parent of the entire Apple group) in the UK, as a related case is already pending in the Northern District of California. Epic Games commented in a statement that it will reconsider pursuing a case against Apple in the UK after the US case is finished.
  Despite (or because of?) the admittedly small setback in the UK, Epic Games took further action against Apple by filing an antitrust complaint against it before the EU Commission as per an announcement. The strategy of Epic Games' global fight against Apple is not obvious, but irrespective of this, the complaint before the EU Commission comes almost two years after Spotify submitted similar complaints about Apple to the EU Commission. As is public knowledge, the EU Commission meanwhile has opened a formal investigation into Apple. The pressure, if anything, is growing.
  Christoph Haid

- **Parallel tariff increases by telecom companies attract the authorities' attention but do not trigger immediate action**
  The Austrian competition authority has received information from whistleblowers

concerning parallel price increases by mobile operators A1, Magenta and Drei, who all plan to increase their mobile and internet tariffs in March. While this might appear to signal collusion, parallel behaviour is allowed. The simultaneous price hikes are therefore not evidence of impermissible agreements restricting competition, which is why the competition authority (as well as the telecom regulator) will take no immediate enforcement action. Market participants having further information on alleged impermissible collusion are referred to the authorities' whistleblowing hotlines. For now, the regulators have invited the telecom companies to a roundtable to explain the situation and safeguard effective competition going forward.
Christoph Haid

- **Surge in ESG initiatives among European venture capital funds**
  While other investment sectors made major pushes into ESG investing way earlier, venture capital funds lagged. ESG stands for "environmental, social and corporate governance", three major factors in measuring an investment's sustainability and societal impact. This includes fundamental principles, from diversity and board structures to labour relations, supply chain, data ethics, environmental impact and legal requirements.
  Over the last several months, quite a few mostly European VCs started to tackle ESG initiatives. In addition, a group of 25 VCs led by GMG Ventures and Houghton Street Ventures formed a community around ESG for VC. The goal is to share their expertise from the bottom up and fill the gap of missing knowledge.
  The two main drivers for this surge in responsible investment are: (i) increasing awareness of activities that may have an influence on external events, such as climate change and social justice; and (ii) increasing awareness of how ESG adoptions can promote targeted business goals, such as increasing sales, recruiting excellence and reducing operational risks.
  Find more detailed information on how VCs and start-ups are influenced by responsible investing here.
  Nikolaus Stepan

For further information, please contact any of the individuals named above, your usual contacts at Schoenherr or any member of our technology & digitalisation group!

Veronika Wolfbauer
Counsel, Austria
v.wolfbauer@schoenherr.eu
T: +43 1 534 37 50791

Anna Katharina Tipotsch
Associate, Austria
a.tipotsch@schoenherr.eu
T: +43 1 534 37 50487

Daria Rutecka
Associate, Poland
d.rutecka@schoenherr.eu
T: +48 22 223 09 23

Dominik Tyrybon
Associate, Austria
d.tyrybon@schoenherr.eu
T: +43 1 534 37 50327

Mina Mihaljčić
Attorney at Law, Serbia
T: +381 11 3202 620
m.mihaljcic@schoenherr.rs

Christoph Haid
Partner, Austria
c.haid@schoenherr.eu
T: +43 1 534 37 50119

Christian Schumacher
Partner, Austria
ch.schumacher@schoenherr.eu
T: +43 1 534 37 50178

Vlad Săndulescu
Attorney at Law, Romania
v.sandulescu@schoenherr.eu
T: +40 21 319 67 90