Security Newsletter

9 November 2020

Subscribe to this newsletter

Folksam data breach leaks info of 1M Swedes to Google, Facebook, more

Folksam, one of the largest insurance companies in Sweden, today disclosed a data breach affecting around 1 million Swedes after sharing customers' personal info with multiple technology giants. The insurer discovered the data breach after an internal audit according to Jens Wikström, Head of Marketing and Sales at Folksam, and reported the incident to the Swedish Data Protection Authority (Datainspektionen).

"The companies that have received personal data from Folksam are, for example, Facebook, Google, Microsoft, Linkedin, and Adobe," Wikström explained. "The purpose has been, among other things, to analyze what information logged-in customers and other visitors searched for on folksam.se." The sensitive personal data shared by Folksam includes various types of info such as social security numbers or that an individual purchased union or pregnancy insurance. "Our purpose with this has been to analyze and give our customers customized offers, but unfortunately we have not done it in the right way," Wikström added.

"We immediately stopped sharing this personal information and requested that it be deleted." Folksam says that there is no evidence at the moment that the shared sensitive data has been used by any third parties improperly. Folksam is one of the largest investors in several big Swedish companies and is one of Sweden's biggest asset managers as the overseer of $50 billion in insurance assets according to Bloomberg.

Read More on BleepingComputer

Even More

Marriott and BA's Reduced Privacy Fines: GDPR Realpolitik

In July 2019, the ICO issued notices of intent to fine BA £184 million ($238 million), and Marriott £99.2 million ($128.2 million) fine. While steep, these proposed fines were nowhere near the maximum possible. With $20.8 billion in 2018 revenue, for example, Marriott faced a maximum possible fine of nearly $840 million. The final fines announced by the ICO are still record-setting for the U.K. But they are also much lower than what was initially proposed - down to £20 million ($26 million) for BA and £18.4 million ($23.8 million) for Marriott.

"The fine reductions have been significant, however, it is important to remember that these were only 'notices of intent' initially and that both were made public by the companies concerned, and not by the ICO." Both businesses responded in detail to the ICO as its investigation continued, and the regulator says each one not only assisted, but has since substantially overhauled its security programs and practices. For BA, the ICO said that the dire economic conditions facing the airline industry had been a major factor in its reducing the fine. For Marriott, the ICO says that the lower final fine more reflects its evolving Regulatory Action Policy, currently under review, which states that "before issuing fines we take into account economic impact and affordability."

The biggest GDPR fine to date has been against Google, which France's privacy regulator CNIL last year hit with a penalty of €50 million ($59 million) for failing to clearly and transparently inform users about how it handles their personal data, and for failing to properly obtain their consent for personalized ads. The second largest GDPR fine came to pass last month, when privacy regulators in Germany slammed clothing retailer H&M with a €35.2 million ($41.2 million) fine for improper workplace surveillance practices.

Final GDPR fines, however, don't necessarily spell the end of potential legal peril for breached organizations. "Quite aside from the precise levels of fine, the notices themselves also serve up a number of key findings of fact, which could form the basis of future civil liability for both organizations and data subjects in the coming weeks and months," privacy attorneys at London-based Mishcon de Reya say in a recent blog post.

Read More on BankInfoSecurity

Even More on ZDNet

Marriott Breach Takeaway: The M&A Cybersecurity Challenge

For organizations looking to buy another organization, fully vetting what's being sold - prior to takeover - would seem to be a business no-brainer. Because once a deal closes, you'll own the organization, IT network warts and all.

That's one major takeaway from an investigation by Britain's Information Commissioner's Office into a massive, four-year data breach suffered by hotel giant Marriott. Or rather, the breach began with hotel chain Starwood's "guest reservation system" in 2014, but went undetected until 2018. Marriott acquired Starwood and its network of hotels - including the Westin, Sheraton, and W brands - in 2016, and thus failed to spot the breach for two more years.

Once you buy it, you own it. The ICO's penalty notice is essential reading for anyone with cybersecurity responsibilities, not least when it comes to M&A activities. The ICO's message: Once you buy it, you own it. "Even if IT vulnerabilities of the target company may not have been properly uncovered during the due diligence process, then upon completion, as acquirer, you will become fully responsible for ensuring cyber resilience of the entire enterprise, including its legacy IT systems and network solutions," privacy attorneys at London-based Mishcon de Reya write in a blog post analyzing the ICO's Marriott penalty.

Read More on BankInfoSecurity

California voters back new data privacy law beefing up CCPA

A state guide for voters describes the proposition, also called the California Privacy Rights Act (CPRA), as a way for consumers to prevent businesses from sharing personal information, correct inaccurate personal information, and limit businesses' use of "sensitive personal information," including precise geolocation, race, ethnicity, and health information. The act would also create the California Privacy Protection Agency.

In a statement, Alastair Mactaggart, chair of Californians for Consumer Privacy and the sponsor of the proposition, hailed it as the "beginning of a journey that will profoundly shape the fabric of our society by redefining who is in control of our most personal information and putting consumers back in charge of their own data." It will force companies to collect only the data they need, limit the retention time of personal information, restrict the further transfer of personal information, and much more.

But now that the proposition has been officially passed and will take effect in 2023, experts are poring through the fine print to figure out how it will be enacted. "Most loyalty card programs I've seen will offer discounts off regular prices to members willing to share their data, while non-members pay the retail price. While this makes sense, a system that would allow companies to charge more for their items would erase any benefit of such a program, as members would likely end up paying retail, while non-sharing customers would pay a premium on top of retail. Being allowed to charge people for the 'privilege' of keeping their privacy is wrong."

Read More on TechRepublic

More #News

- Hackers have only just wet their whistle. Expect more ransomware and data breaches in 2021.
- Scam PSA: Ransomware gangs don't always delete stolen data when paid
- Malicious npm package opens backdoors on programmers' computers
- Prioritizing Vulnerability Response with a Stakeholder-Specific Vulnerability Categorization
- Maze Claims to End Its Ransomware and Extortion Operations
- Premium-Rate Phone Fraudsters Hack VoIP Servers of 1200 Companies
- New NAT/Firewall Bypass Attack Lets Hackers Access Any TCP/UDP Service
- Rackspace Hosted Email Flaw Actively Exploited by Attackers
- GitHub denies getting hacked
- 23,600 hacked databases have leaked from a defunct 'data breach index' site
- Google Patches 30 Vulnerabilities With November 2020 Android Updates
- SaltStack reveals new critical vulnerabilities, patch now
- CERT/CC Seeks to Remove Fear Element From Named Vulnerabilities
- Blackbaud sued in 23 class action lawsuits after ransomware attack
- If you want security, lie to me
- Toy maker Mattel discloses ransomware attack
- Why Paying to Delete Stolen Data is Bonkers

#Patch Time!

- Cisco discloses AnyConnect VPN zero-day, exploit code available
- Oracle issues emergency patch for critical WebLogic Server flaw
- Hacking Group Targeted Zero-Day Flaw In Oracle Solaris
- Patch for Critical VMware ESXi Vulnerability Incomplete
- Another Chrome zero-day, this time on Android – check your version!
- Adobe fixes critical security vulnerabilities in Acrobat, Reader
- Update Your iOS Devices Now — 3 Actively Exploited 0-Days Discovered

#Tech and #Tools

- Infection Monkey - Data center Security Testing Tool
- Intercepting HTTPS on Android
- Github: Widespread injection vulnerabilities in Actions
- A Practical Introduction to Container Security
- "Kubernetes from an Attacker's Perspective"
- Ryuk Speed Run, 2 Hours to Ransom
- Attacks on industrial enterprises using RMS and TeamViewer
- Assemblyline 4: open source malware analysis platform
- MalwareMultiScan: Self-hosted VirusTotal / OPSWAT MetaDefender wannabe API
- Implement password-less authentication with Amazon Cognito and WebAuthn
- AWS Nitro Enclaves: Additional isolation to further protect highly sensitive data within EC2 instances
- How to Prevent Pwned and Reused Passwords in Your Active Directory

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

https://news.infosecgur.us