ComputerWeekly.com | TechTarget

E-guide

CW+ Content

CIO Trends #10: Nordics

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

In this e-guide:

Swedish people are pioneering when it comes to adopting the latest technologies. For example citizens of the Nordic country are some of the most fervent users of mobile banking, so much so that Sweden is predicted to be one of the first cashless, or at least near cashless, societies.

But this malleability to new tech has its limits. Read in this e-guide how Swedish consumers are losing confidence in social media, with increasing distrust over personal data use and online privacy.

But the Swedish will continue to innovate in adopting tech for business and social challenges. Also in this issue read about how one Swede created a platform to support cancer sufferers after blogging about his own fight proved valuable to others.

Karl Flinders, EMEA content editor

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Survey about Swedish people's attitude to the internet reveals growing distrust of social media

Gerard O'Dwyer

Public confidence in global social media operators Facebook and Google retreated in Sweden in 2019 amid growing public distrust over personal data use and online privacy.

The "trust factor" contributed to a decline in Facebook's popularity in Sweden in 2019, according to a survey conducted by Internetstiftelsen (Internet Foundation Sweden), the public service organisation tasked with ensuring the positive development of the internet in Sweden.

The Internetstiftelsen survey, *Swedes and the internet 2019* (in Swedish, *Svenskarna och internet 2019*) revealed that public confidence in social media giants Facebook and Google declined by 17% in Sweden from 2015 to 2019. The annual survey is a useful tool to measure online behaviour in Sweden as well as societal changes in the face of increasing digitalisation.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Sweden is among the most digitalised of the Nordic countries. More than 98% of Sweden's households are connected to the internet, while access to fibre increased to 57% of homes during the fourth quarter of 2019.

Just 25% of Swedes surveyed in Internetstiftelsen's report considered the time they spend on social media platforms to be "meaningful".

By contrast, 60% in the survey felt that time spent on various domestic and international news apps was a meaningful use of their time. The corresponding figure for time spent playing online and mobile games, by comparison, was just 12%.

In 2019, 91% of Swedes used their personal computers to access the internet, the Internetstiftelsen survey found. More than 90% of Swedes accessed the internet using Android and smartphone devices, while 61% used tablets.

According to the survey, more Swedes are now "taking a closer look" at how their personal data is being used, not just by technology giants such as Google and Facebook, but more generally by state organisations and public authorities in Sweden. The primary concern for consumers relates to possible intrusions into their personal privacy online.

"Almost half of all Swedes feel monitored on the internet. There is a trend whereby they are becoming more restrictive when it comes to sharing other people's posts on social media. Overall, we are seeing that the use of social

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

media seems to have begun to level off," the Internetstiftelsen survey-based report states.

Significantly, the Internetstiftelsen survey reveals that while around 50% of Swedes are worried that leading social media actors such as Google and Facebook may be infringing on their privacy and failing to adequately protect their personal data, less than 26% have the same fears about government organisations and public authorities.

"What the survey reveals is that more Swedes are becoming increasingly worried that large companies like Facebook and Google are infringing on their personal privacy online," said Måns Jonasson, director of digital strategy at Internetstiftelsen.

"I think the Cambridge Analytica scandal, and the many notable hacking attacks that have taken place over recent years, has caused people to reflect about how they spend their time in the internet and social media space."

The Internetstiftelsen survey reveals that Swedes are very much at home in being part of the evolving digital society.

Although the general trend is one of unease over how private and public organisations are invading privacy and using personal data, a majority of Swedes embrace change and the development of digital e-services within defined public service areas such as healthcare, transport and mobile banking.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

The decline in Facebook's popularity in Sweden is unlikely to have a consequential impact on public trust and confidence in e-commerce, said Per Ljungberg, the CEO of Svensk Handel, the central organisation for the country's trade and business sectors.
"Consumers' loyalties change. If consumers don't like a certain platform, they will move to another. For e-commerce, there are always multiple channels to use. Should consumers lose confidence in Facebook or Google, they will simply go elsewhere. However, I don't see this happening right away, and there are no indications that this will happen in the near future," he said.

Svensk Handel's own research, coupled with feedback from the business and industry employers organisations that it represents, reinforces the view that the "digital power momentum" has shifted to consumers, said Ljungberg.

"The power has definitely shifted to the consumer in digitalisation. Most visibly, this has changed the security aspect of e-commerce. Today's e-retailers must be able to respond to how the individual's data is used, what data legislation requires of them in terms of taking responsibility for complying with GDPR [General Data Protection Regulation] rules," he said.

The growing skepticism being experienced by Swedes with the leading media platforms is compounded by the "targeted ads fatigue factor", said Jonasson. Consumers are becoming less tolerant of targeted advertising online. This has become a major source of annoyance that builds hostility and suspicion towards media platform operators, he added.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"A consumer running a simple Google search in the morning can result in recurring advertising for a specific product for the rest of the day on Facebook. Consumers are growing tired of targeted advertising online.

"The strength of Google and Facebook is being able to deliver that personalised touch. Consumers don't always appreciate how this is done. The working models of social media platforms will likely become more data-driven, not less, in the future," Jonasson said.

Although the Internetstiftelsen survey observes a decline in Facebook's popularity in Sweden, Jonasson believes that the development could be an adjustment rather than signalling an irreversible trend.

"While there is a decline in Facebook's popularity in Sweden, it is a marginal slide in interest, and it's a trend that is happening for the first time. Interest in Facebook may have peaked in Sweden, yet no alternatives really exist to replace it right now.

"It is possible that smaller social media networks will appear that are more niche, or maybe the Web might return to how it was in the 1990s. To this extent, only time will tell what the future holds," said Jonasson.

The Internetstiftelsen survey also provides credence to the widely held perception that the introduction of data protection legislation, including the

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

GDPR, hasn't made consumers any more cautious about providing personal data to social media platforms and their services' offerings.

Most internet users in Sweden still accept the terms of use on social media platform sites without carefully reading through the terms and conditions. The Internetstiftelsen survey also reinforces the general view that older social media platform users tend to be more knowledgeable about personal data protection.

Consumers 55 years and above are also likely to be more attached to older forms of communication such as email, Skype and Facebook Messenger, while younger users gravitate more freely towards WhatsApp, Snapchat, Instagram and video-calls.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Personal transport as a service drives across Nordics

Alex Cruickshank

The Nordics could see a pan-regional platform that enables citizens to access personal transportation on demand as the market for mobility-as-a-service (MaaS) expands.

Towards the end of last year, a consortium of Nordic mobility companies and transport-related organisations announced a project aiming to unify the region's MaaS market.

And with a general shift away from personally owned transportation and towards mobility provided as a service, these schemes are gaining traction.

The aim of MaaS is to provide the most appropriate transport method to any traveller or commuter as and when they need it, eliminating, or at least reducing, the need for individual ownership of, or subscription to, any particular method of transport.

The new project, the Nordic Mobility Innovation Platform (NMIP), has the stated goal of creating open technology and business practices for MaaS and smart

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

mobility services. Although the scheme is starting in the Nordics, the intention is for the resulting technology and practices to be relevant globally.

Coordinating NMIP is Finnish smart mobility platform company Kyyti Group, which is working alongside Nordic-based intelligent transport system (ITS) organisations ITS Norway, the Capital Region of Denmark, Swedish MaaS operator UbiGo, and research centres RISE in Sweden and TØI in Norway.

"Collaboration in the Nordics can have a global impact," said Trond Hovland, managing director of ITS Norway. "The MaaS standards developed today may make the way people move significantly more convenient in the future, in the Nordics and beyond."

Pekka Niskanen, COO of Kyyti Group, said the current status of MaaS in the Nordics is seeing initiatives popping up all the time and the concept is growing rapidly. "The private and public sector are both interested and the first MaaS operations are typically still in piloting mode," he said. "However, these initiatives are still very local and the range of services they include varies tremendously."

For this reason, the first stages of NMIP will focus on working out the initial use cases in the Nordics – which groups would benefit from the project. Based on those findings, the consortium plans to establish a MaaS roaming pilot, which will feed input into efforts to define a market enabler framework, with the aim of creating a single, open mobility framework for the region.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Niskanen added: "It will require work to define implementation guidelines for standardisation and recommendations for pan-Nordic datasets and APIs [application programming interfaces]. We will establish a venue for knowledge-sharing and collaborative innovation, in which there is already huge interest from the US to Japan, various European countries and industry associations such as the MaaS Alliance."

Standardising MaaS

Rather than trying to reinvent the wheel, the NMIP consortium will collaborate with existing international MaaS initiatives, including the MaaS Alliance, which is a public-private partnership that aims to standardise MaaS, which it defines as "the integration of various forms of transport services into a single mobility service accessible on demand".

The MaaS Alliance says: "To meet a customer's request, a MaaS operator facilitates a diverse menu of transport options, be they public transport, ride-, car- or bike-sharing, taxi or car rental/lease, or a combination thereof. For the user, MaaS can offer added value through use of a single application to provide access to mobility, with a single payment channel instead of multiple ticketing and payment operations. For its users, MaaS should be the best value proposition, by helping them to meet their mobility needs and solve the inconvenient parts of individual journeys as well as the entire system of mobility services."

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

With that goal in mind, the Netherlands is of particular interest to NMIP project, because that country is already at an advanced stage of MaaS standardisation. Niskanen said: "We are an open project and gladly work with different projects to know what is being done elsewhere, in order to avoid doing the same work twice."

Progress is already being made in implementing MaaS in the Nordics, for example the world's first nationwide MaaS offering in Finland for Matkahuolto, a provider of inter-city passenger and parcel transportation services. NMIP intends to make use of Matkahuolto's nationwide MaaS operation as a stepping stone to initiate its own MaaS roaming pilot by the summer of 2020.

And as recently as December, it was announced that the Swedish city of Linköping will start providing a full-blown MaaS service this summer through a public/private collaboration. This will be implemented using Kyyti's own MaaS platform, further consolidating the concept of a core Nordic approach to MaaS.

According to a recent presentation by Kyyti, the next steps for NMIP are as follows:

- ITS Nordics has agreed on collaboration with the ODIN project and a joint workshop has been held to initiate shared work on Nordic standards and guidelines.
- The research institutes RISE and TØI are starting to define pan-Nordic use cases to reflect real-life mobility challenges for future field tests.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

- Kyyti and UbiGo are initiating work to define an implementation plan for cross-national MaaS roaming proof of concept, building on use cases and standards.
- The Capital Region of Denmark is working on a knowledge-sharing environment to engage the various parties that have already shown interest in the project.

Ultimately, the intention is to have a single market framework covering multiple Nordic cities. For example, whereas today a traveller in Stockholm may use a different MaaS framework and market operator to a traveller in Copenhagen, in the future, both travellers, despite using different market operators, will tap into the same underlying MaaS framework.

It is this market enabler framework that NMIP intends to provide – a single point of access for market operators, aggregating transport systems from train to bus, tram to car, bicycle to ferry, car-sharing to e-scooter, to any other form of commuter transport imaginable. The project's short-term goal is to demonstrate the concept's viability, after which market forces should take over.

In the long term, it is hoped that this example will inspire and create a set of standards and business practices that will work anywhere. Scalability is key for NMIP. Today the Nordics, tomorrow the world – or at least the rest of Europe.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack

Bill Goodwin, Investigations Editor

Travelex said today that it was to begin restoring its IT systems, which provide electronic foreign exchange services to banks and its own branch network, nearly two weeks after the company was hit by cyber gangsters.

The company faced a $6m demand from a cyber mafia group to decrypt its internal files after discovering its networks had been attacked by Sodinokibi malware - also known as REvil - which disrupted the company's operations in nearly 70 countries.

The attack has left more than a dozen banks in the UK, including the Royal Bank of Scotland, NatWest, First Direct, Barclays and Lloyds, which rely on Travelex to provide services, unable to provide foreign exchange services.

Banks in Australia, including NAB, the Commonwealth Bank and Westpac, have also been hit by the attack.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Travelex said today that it had restored some of its internal order processing and was starting to restore customer-facing systems, beginning with in-store computer systems used to process electronic orders.

"We are now at the point where we are able to start restoring functionality in our partner and customer services, and will be giving our partners additional detail on what that will look like during the course of this week," said Travelex CEO Tony D'Souza.

The company declined to say whether it had paid a ransom to the cyber criminals that disabled its global networks - a move that would allow it to recover encrypted files on computers in Travelex stores and offices worldwide.

It is unclear whether Travelex has back-ups of the encyrpted files, which include the names of clients and bank account and transaction details, according to people familiar with Travelex.

Hackers threaten Travelex on dark web

Last week, Computer Weekly reported that the Sodinokibi crime syndicate had threatened to sell Travelex customers' credit card details and personal data on the dark web.

It emerged today that the criminals behind Sodinokibi have released internal documents from another hacked company – US Computer Services firm, Artech – which was hit by a similar ransomware attack in late December 2019.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

The hackers have posted a message on an underground hacking forum, threatening to disclose further hacked information from Artech, which claims to be the largest IT staffing company owned by women in the US, unless the company agrees to pay an undisclosed ransom.

Irina Nesterovsky, head of research for Israeli security company and specialist in darknet threat intelligence, Kela, which identified the post, said it marked a significant change of tactic for the crime group, which first appeared in April 2019.

"This is the first time that the group behind Sodinokibi published alleged proof of their attack," she said. "While not mentioning explicitly Travelex – this is definitely a nod towards them and any other company that would be attacked by the operators of the ransomware, and refuses to pay."

Travelex said it had found no evidence that its customer data had been stolen.

Travelex staff ordered to return laptops

Travelex has instructed employees to hand over their laptop computers to IT specialists for analysis, according to people familiar with the attack.

The company is categorising laptops as red, amber or green, depending on the risk they pose to the organisation and the damage caused by the malware.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"IT teams will contact you as soon as they are able to rebuild your device," said instructions sent to Travelex staff.

Those with unaffected computers have been told to keep their machines switched on and connected to the internet, so the computers can receive continuous updates and be monitored for suspicious activity.

Problems persist with payroll

The incident has disrupted employees' ability to access the company's Workday HR system, which is hosted in an independent cloud service.

People familiar with the situation told Computer Weekly that staff were only able to access basic functions HR functions.

Some staff have been told they will receive estimated salaries, as the company has not been able to update payroll systems with details of their overtime during the crisis.

"This has impacted many staff who worked extra hours and holidays over Christmas and the New Year and haven't been paid for it," one member of staff said.

Staff who received too much have been asked to pay back Travelex once its IT systems are back up and running.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Staff implement manual workarounds

Computers and point-of-sale machines in Travelex's retail outlets are still out of action, forcing staff to use cash books to keep track of transactions.

Customers are being told they can only buy foreign exchange with cash as the company is unable to process card payments.

Employees have been asked to use their own mobile phones to communicate with the company, and have set up WhatsApp groups to receive updates from managers.

"Staff are pulling together. We all realise we've only got each other to rely on to get through this," one person told Computer Weekly.

"Older staff have found the transition to pen, paper and calculator easier, but younger employees have taken time to adjust. The younger ones are starting to find their feet and getting more confident, but many cannot grasp the concept of doing a manual balance at the end of the day," they said.

Travelex plans recovery roadmap

Travelex said in a statement today that it would continue to communicate with partners about the resumption of services and provide a roadmap setting out the next steps in its recovery.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

It said the company had been able to honour "most" online orders for collection in store and, where it could not, it has proactively reached out to people affected to make alternative arrangements, through its 24/7 customer support desks.

But one person familiar with the attack said communications had been chaotic.

"We're receiving updates on procedures and the latest story to give to our customers every couple of days, and every time they change their minds on what we are supposed to do. They seem to be making it up as they go along," the person said.

Travelex warns staff not to comment on attack

Travelex has sent its employees pre-prepared speaking notes to repeat to customers when asked questions.

The company has also warned staff to say "no comment" to journalists. Travelex has instructed employees to take the name of any reporter asking questions, along with their contact details and organisation, and pass the information on to line managers.

Managers have also instructed employees to report any unusual calls or suspicious visits by people to Travelex counters.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Warning to Travelex

Kela's Nesterovsky said the decision by hackers to not to disclose Travelex internal company information, unlike that of Artech, might imply that Travelex has negotiated with the cyber crime group.

"The fact that no documents from Travelex were published yet could hint to the fact that the company has gotten in contact with them. Another option is that the data stolen from Travelex is more sensitive in nature, and they would not share it in public like that," she said.

Analysis by Computer Weekly of Artech files released by Sodinokibi hackers appears to show that hackers had widespread access to the company's internal networks, including administration credentials which could have provided administrator-level access.

The Information Commissioner's Office (ICO) said Travelex had not reported an information breach.

"We are in contact with Travelex and giving advice on potential personal data issues following the recent ransomware attack. The company has not reported a data breach," said an ICO spokesperson.

"If an organisation decides that a breach doesn't need to be reported they should keep their own record of it, and be able to explain why it wasn't reported if necessary," said the spokesperson. "Organisations must notify the ICO within

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

72 hours of becoming aware of a personal data breach unless it does not pose a risk to people's rights and freedoms."

A spokesperson for the Financial Conduct Authority, which regulates Travelex, said: "We are aware of the issue and in contact with the firm to ensure affected customers are treated fairly."

Ransom demands

Computer Weekly reported that Travelex had been attacked by ransomware in a report on 3 January and identified the origin of the attack as Sodinokibi on 6 January.

Sodinokibi subsequently told security web site Bleeping Computer that the group had accessed 5GB of information from Travelex and had threatened to publish sensitive information, including credit card details and social security numbers, unless Travelex paid a $3m ransom.

The group went on to tell the BBC that it was demanding a $6m ransom, and would release sensitive customer data by 16 January unless Travelex paid-up.

Update: 14 January 2020

A spokesperson for Artech confirmed to Computer Weekly that the company's computer systems had been hit by a malware attack on the morning of 8 January.

"As a precaution, we immediately shut down all of our systems in order to fully investigate the attack and ascertain whether any sensitive or personal data was compromised. While we will continue to conduct further forensic examination, at this stage we believe that no sensitive or personal data has been compromised," the spokesman said.

Additional research by Matt Fowler.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield

Bill Goodwin, Investigations Editor

The European Court of Justice (ECJ) has backed lawyer and privacy activist Max Schrems and Facebook in a legal opinion which found that the contractual agreements widely used by companies to share data between the European Union (EU) and the US are lawful.

Advocate general Henrik Saugmandsgaard Øe said the agreements, known as standard contractual clauses (SCCs), were valid under EU law as mechanisms for ensuring the privacy rights of EU citizens are protected when their data is transferred overseas.

But he raised questions over the lawfulness of the EU-US Privacy Shield agreement on data protection in the light of evidence that the US runs bulk surveillance programmes which breach European privacy laws and fail to give European citizens adequate rights of redress if their data is wrongly intercepted.

The case originates in 2013, when Schrems complained to the Data Protection Commission Ireland that Facebook was providing "mass access" to data on its

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

European customers to the US intelligence agencies, in breach of European privacy law.

Speaking today, Schrems said he was generally pleased with the court's statement. "The opinion is largely in line with our legal opinion and is an important sign of protecting the privacy of users," he said.

In a 97-page legal opinion, Saugmandsgaard Øe found that US bulk surveillance programmes did not mean that standard contractual clauses, which are used by more than 100,000 companies to share data with the US, were unlawful.

But he said there was an obligation by national data protection supervisors – in this case Irish data protection commissioner Helen Dixon – to investigate complaints about breaches in European data and to take action if the transfers fail to meet EU law.

"Where appropriate, [the supervisor] must suspend the transfer if it concludes that the standard contractual clauses are not being complied with and that appropriate protection of the data transferred cannot be ensured by other means," wrote Øe.

Questions over Privacy Shield validity

The Advocate General found that although the European Court of Justice did not need to make a decision on Privacy Shield, there were questions

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

over whether Privacy Shield gave adequate privacy rights to EU citizens when their data is shared with the US.

He said that Dixon should be given the chance to re-examine her files in the case. If she considered that Privacy Shield was an obstacle to her powers to suspend Facebook's transfer of data to the US, it would be open to her to bring the matter before the national courts to refer back to the ECJ.

"Prudence dictates that the court should await the completion of these procedural steps before it examines the impact which the Privacy Shield decision has on the way in which a supervisory authority deals with a request to suspend a transfer to the US," he said.

Saugmandsgaard Øe said the validity of the Privacy Shield decision depends on whether the US ensures an "essentially equivalent" level of protection to EU data to that guaranteed by the General Data Protection Regulation (GDPR), the European Charter of Fundamental Human Rights, and the European Convention on Human Rights.

But according to the Advocate General's opinion, it is not certain that US bulk surveillance programmes – authorised by section 702 of the Foreign Intelligence Security Act and Executive Order 12333 – provide adequate levels of privacy for EU citizens under EU law.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"I have doubts about the validity of the finding that the US guarantees, in the context of their intelligence services…and adequate level of protection," he said.

A relief for European businesses

The case is expected to be heard by the European Court of Justice next year. In the majority of cases, the ECJ follows the opinion of the Advocate General, though some people involved in the case believe the court may reach a different finding.

Lisa Peets, the lawyer at Covington and Burling representing the Business Software Alliance, which was joined to the case, said the Advocate General's decision to affirm the validity of SCCs was "tremendously important for companies across the economy, which rely on the SCCs for many of their day-to-day operations".

Richard Cumbley, partner at Linklaters, said: "The Advocate General's decision will prompt a huge sigh of relief amongst European businesses that deal with affiliates or suppliers in the US."

He said the decision meant that businesses could use standard contractual clauses as a mechanism to share data with Europe following Brexit.

"They will therefore be an important tool for UK businesses to receive data from the EU post-Brexit, and make an adequacy finding a desirable rather than critical aspect of the forthcoming trade negotiations."

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Graham Doyle, head of communications for the Irish Data Protection Commission, said that opinion raised important issues. They include that EU law applies when a person's data is processed by public authorities outside the EU, that US laws and practices lead to interference with the rights of individuals that are incompatible with US law, and that those problems are not cured by Privacy Shield.

"The opinion illustrates the levels of complexity associated with the kinds of issues that arise when EU data protection laws interact with the laws of third countries," he said.

Antony Walker, deputy CEO of trade group TechUK, said Saugmandsgaard Øe's opinion was particularly important for small businesses preparing for Brexit, but he said there was still uncertainty over Privacy Shield.

"The Advocate General questioned the validity of Privacy Shield on the right to respect for private life and the right to an effective remedy. There will be a lot of focus on how these questions are addressed by the final CJEU [Court of Justice of the European Union] ruling," he said.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Finnish government supports local authorities in cyber security initiative

Gerard O'Dwyer

The Finnish government is providing technical and financial support to an IT and cyber security initiative being run in partnership with the country's municipal districts.

Over 200 of Finland's 311 municipalities have joined the Local Government Anti Cyberspace Threats (LGACT) project to conduct joint IT network defence exercises. The project will share information on strengthening municipal IT systems against a broad range of malicious attacks from the cyber domain.

The LGACT, which ran a major multi-agency joint exercise in November, will also serve as a collaborative platform and professional skills hub to test cyber risk-related predictive software. Moreover, the LGACT will cooperate with the state's leading cyber and national security organisations to develop a range of defensive and offensive tools that reduce risk exposure to next-generation threats and attacks from cyber space.

The November cyber exercise saw the LGACT collaborate with the National Cyber Security Centre (NCSC), The Association of Finnish Local and Regional

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Authorities (Kuntaliitto), The Population Register Centre of Finland (PRCF/Väestörekisterikeskus) and the state IT security agency VAHTI (Valtionhallinnon Tieto- ja Kyberturvallisuuden Johtoryhmä) to run the Taisto-19 (Battle-19) cyber security exercises.

As part of the Taisto-19 drill, the coordinating agency, PRCF, assumed the role of "bad actor" to launch a hostile simulated ransomware-style attack against municipalities' IT networks. The "hacker" demanded payment in bitcoin by a defined date and issued a ransom demand threatening to infect primary IT networks with malicious malware. The "hacker" warned it would unleash "highly destructive malware" created to cause irreversible systems failure at a significant financial cost to the local government authorities.

"Exercises like Taisto 19 are becoming increasingly relevant in a world where cyber attacks against government IT networks are more common," said Kimmo Rousku, the director general of VAHTI. "We are seeing enthusiasm from municipalities to apply what they learn in these cyber defence exercises. The goal is to improve the security of IT networks and core operating systems."

Operating as a department of the Ministry of Finance, VAHTI is the Finnish state's chief government information and cyber security steering group.

VAHTI's elevated role since 2018 has seen the agency become more engaged in projects to support the integration of information and cyber security, ICT preparedness, administrative operations, management and performance

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

management. In the cyber security sphere, the expertise being provided by VAHTI embraces a higher focus on cryptocurrency ransomware-type threats.

Response to real attacks

The Taisto-19 exercise took place against the backdrop of the high-profile cyber attack against the city of Lahti in June. The malware attack infected and compromised over 1,000 computer workstations across the public authority's health, public utilities, education and administrative services departments.

The cyber attack against Lahti, which is being investigated by Finland's National Bureau of Investigations (NBI) in cooperation with the NCSC, has resulted in a broader probe to ascertain the actual scale of attacks by cyber domain bad actors against public services websites and IT infrastructure in 2019.

The NBI itself, along with ether public bodies, became the target of a more general distributed denial-of-service (DDoS) cyber attack on 21 August. The force of the DDoS attack, by unidentified hackers, caused widespread server functionality failures that, in some cases, disrupted normal service on targeted websites for over two days.

The NCSC and the NBI have also rolled out a new cyber security initiative to deepen their professional collaboration with organisations across the public and private sectors.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

The criminal purpose, and growing sophistication, of new cyber threats presents significant challenges for both the state and the private sectors in protecting critical IT infrastructure, said Antti Pelttari, the head of the Finnish national security intelligence service, SUPO.

"The extreme threat is that critical infrastructure could end up in the control of a state conducting active cyber espionage. Likewise, cyber influencing constitutes a threat to national security. Steps to secure IT networks and IT critical infrastructure must take account of measures to protect the integrity of 5G-related projects and investments in future 5G networks," said Pelttari.

Building cyber security expertise

Finland strengthened its cyber security defence apparatus in October when it bolstered measures contained in the National Cyber Security Strategy 2019. The resulting reform creates three strategic guidelines. These include international cooperation, improved coordination of cyber security management, planning and preparedness, and the accelerated development of cyber security competence.

The reinforcement measures are in the National Cyber Security Strategy 2019 (NCSS-2019) which are required to align Finland more closely with the European Union's Cyber Security Strategy.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

On a practical level, the NCSS-2019 includes increased spending provisions to channel more funds and professional expertise to fundamental areas such as cyber defence and offence competence. Additional resources will be made available to the NCSC to sharpen its ability to conduct 24/7 situational awareness and liaise more effectively with public authorities and the business sector.

Finland is also strengthening international cooperation as part of its multi-tiered approach to strengthen its national cyber security infrastructure. Finland's Ministry of Defence (MoD) hosted a Cyber Ranges Exercise in Helsinki in October that showcased the European Defence Agency's (EDA) Cyber Ranges Federation.

The EDA project provides a testing platform for 11 European member states to pool national cyber ranges expertise. The primary shared ambition is to support member states in their push to improve their respective cyber defence training capabilities.

The EDA's Cyber Ranges Exercise event featured a live fire exercise based on a fictive but realistic training scenario. In this format, country teams were challenged to respond to, and defend against, cyber attacks launched by other country teams. The exercise used a software-defined wide area network (SD-WAN) as the backbone network technology. All participating national cyber ranges were interconnected and interacting in real time, each tasked with a specific role to play in the exercise.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"International cooperation is critical to enable individual countries like Finland to become active and effective players in the cyber domain. It is important that we continue to develop the scope of cooperative projects like the Cyber Ranges Federation platform going forward," said Jukka Juusti, the Finnish MoD's permanent secretary.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Swede's war on cancer moves to a digital battlefield

Matthew Staff, Contributor

When Fabian Bolin fell ill in his native Sweden back in 2015, the former investment banker and actor didn't know he was about to begin a war. First came his personal battle against leukaemia, which he eventually won. But beyond that, his subsequent tech startup enterprise has made waves across the medtech scene as he continues his wider War On Cancer platform.

The aptly named app primarily serves as a social media portal for people with cancer, and for their families and friends, to share stories and experiences as part of the lesser talked-about mental health side of the disease. From there, the app has also evolved into a progressive tool that is now looking to fill other gaps in the healthcare proposition, leading to its current role as a data-driven facilitator of future cancer breakthroughs, treatment and care.

"It all started with a blog," said Bolin, alluding to some of his darkest days during his treatment and recovery phase. "It became my own saviour from a mental health perspective to share my experiences," he said. "Storytelling as if it were a diary, but sharing so intensely and openly that I inadvertently created a powerful

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

tool that started being read and shared by people in a similar situation to me around the world.

"I soon realised it was helping others, and that had the most profound impact on my mental wellbeing. I've never had more of a purpose realising that my experiences were making people feel the way they did, and I realised that this concept could be scaled on a global level."

Having always had an entrepreneurial mindset, Bolin got to work with friend Sebastian Hermelin to convert storytelling into a socially-driven mental health tool, and the first version of War on Cancer was launched in May 2016.

Tapping into the advent of medtech as a trend and sub-sector, the pair were soon being invited to some of the biggest healthcare conferences in the world, where, in turn, some of the biggest heavyweights in tech and medicine threw their support behind the model.

"They saw how disruptive War on Cancer could be in a clinical setting, from both a healthcare and life sciences point of view," said Bolin.

"By uniting the world in this one app, we were pointed towards the significance of data generation, as well as the social and mental benefits we had earmarked. Real-world evidence, data, clinical trial matchmaking, patient understanding – all these parameters that traditional institutions would pay insane amounts of money to collate and organise and try to turn into tangible progression.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"We saw we could now become this dynamic provider through the ecosystem we had built and, while we are still working out how best to do this, we are excited about the potential outcomes."

Purposeful data

This take on data's potential is what makes War on Cancer unique, outside of its core storytelling and social function.

Traditional healthcare has often kept patients in the dark when it comes to encouraging people to take part in trials, surveys or research – the foundations of clinical data. But Bolin realised that this actually goes against human impulse, and was hindering the collation of more comprehensive datasets.

"You see it now with blood donations, for example," he said. "People get a message when their blood has been used, telling them where it has and to what extent. It makes people euphoric to know they have helped. It's not the data-sharing itself that they're uneasy with, it's the fact that they don't know what it's being used for or what the end result is.

"In 2020, what we're looking to facilitate through a separate app feature called Track Your Impact is the option for individuals to contribute to different clinical trials, university studies or hospital surveys. It's essentially a matchmaking tool where the healthcare arm has to stipulate what the data will be used for and to

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

keep participants updated on this process, and the participants can choose at that moment whether to get involved or not."

In providing people with this outlet, War on Cancer is encouraging that same feeling of wider purpose and collaboration that Bolin felt when he first began writing his blog. People want to help others, and now have a user-centric platform to do so in what is traditionally a tech-unfriendly domain.
Bolin added: "It sounds odd, but it brings a sense of reason to having cancer. It's a horrible question you're faced with – 'why me?' – and this almost offers an answer, and gives people some control over a situation that often controls you."

Filling the gaps in healthcare

It begs the question as to why traditional healthcare institutions have not explored such solutions already – but it is actually this question that informs the need for an app like War on Cancer.

For generations, the idea of in-hospital healthcare could be better labelled as survival. Doctors and hospitals are tasked with keeping people alive, but don't always have the resources or inclination to tick off every stage between admission and discharge.

"It's understandable that they think this way as it's their job, but it doesn't mean they should be so resistant to outside help or the idea of partnering with organisations that can fill in the gaps when it comes to overall care," said Bolin.

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

"I was being cured while in hospital, but many of the concerns I actually had day to day were going unanswered.

"What could I eat, when would I be strong enough to start doing exercise, just generally why was I feeling so down one day and then fitter the next? All of these hour-by-hour challenges can't be addressed by hospitals for every patient, and that's why digital platforms such as ours can be so vital."

There are signs of progression to this end. In the UK, War on Cancer is already in discussions with the NHS to be added to its app library, a source of relevant digital tools that help to advise and care for individuals in a more personalised, relatable way.

"There's a long way to go in general, though," said Bolin. "When money is available for investment, it inevitably, usually, goes towards people or medical equipment before digital innovations away from the treatment table or hospital bed.

"Healthcare institutions aren't tech companies at heart, and so they don't have the competence or funds to build something like War on Cancer internally, but are still reluctant to look towards collaborations to fill these gaps instead."

From gods to guides

Bolin noted that healthcare as an industry is transforming, but still needs more of a shift. It signals the need for a transcendence among medical professionals,

from “gods to guides”, he said – a theory that traditional medical professionals are not always happy with.

“They don’t want to sit with patients and go through apps like guides,” said Bolin. “They just want to save lives, like gods. But that’s how healthcare needs to progress given the vast, diverse requirements that patients have – especially with something like cancer.

“By bridging the social side for mental health and day-to-day guidance, and the data side for longer-term improvements, we hope we are furthering a conversation around healthcare going beyond just saving lives, to actually making people’s lives better.”

In this e-guide

- Survey about Swedish people’s attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after ‘Sodinokibi’ attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

In this e-guide

- Survey about Swedish people's attitude to the internet reveals growing distrust of social media
- Personal transport as a service drives across Nordics
- Travelex to begin restoring foreign exchange services two weeks after 'Sodinokibi' attack
- EU court opinion finds EU-US data transfers lawful but raises questions over Privacy Shield
- Finnish government supports local authorities in cyber security initiative

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com