RECENT DEVELOPMENTS IN PRIVACY

JUNE 2022

Weil

THE UK'S INTERNATIONAL DATA TRANSFER AGREEMENT AND THE ADDENDUM IN FORCE

SUMMARY

On 21 March 2022, following parliamentary approval, the:

- International Data Transfer Agreement ("**IDTA**"), which legitimises data transfers from the UK to jurisdictions other than the EEA (and that have not benefitted from an adequacy decision); and
- international data transfer addendum to the EU standard contractual clauses for international data transfers ("**Addendum**"), which is to be incorporated alongside the New EU SCCs (defined below) for data transfers from the UK to the EEA, entered into force.

For international data transfers to be lawful, appropriate safeguards must be implemented. To satisfy this, many organisations rely on the EU's Model Clauses, known as the standard contractual clauses ("**SCCs**"), which impose contractual obligations on data importers and data exporters. On 7 June 2021, the European Commission published a new version of the SCCs ("**New EU SCCs**"), which apply to data transfers from the EEA to jurisdictions outside of the EEA, to address deficiencies in the old SCCs ("**Old EU SCCs**"). As a consequence of the UK having left the EU, the New EU SCCs do not apply to data transfers from the UK to jurisdictions outside the EEA. As such, prior to the IDTA and Addendum entering into force, UK organisations were required to continue to rely on the Old EU SCCs.

THE IDTA AND ADDENDUM

The IDTA may be used as a standalone agreement or incorporated into a commercial agreement. Similar to the New EU SCCs: the IDTA addresses deficiencies in the Old EU SCCs, such as the impact of the Court of Justice of the European Union's ("**CJEU**") judgment in *Schrems II*, which invalidated the EU-US privacy shield; and requires data exporters to undertake transfer risk assessments to consider local laws, practices, and risks which may render the IDTA's protections insufficient. However, the IDTA departs from the New EU SCCs in a number of ways, for example it:

- recognises that parties may have entered into a separate commercial agreement (the "**Linked Agreement**") and allows parties to incorporate the terms of the Linked Agreement into the IDTA;
- enables parties to resolve disputes arising out of or in connection with the IDTA through arbitration;
- allows parties to agree on audit (subject to certain conditions)
- does not adopt a modular structure; and
- imposes reduced obligations on the importer in some circumstances. For example, where a data breach occurs, the IDTA only requires the data importer to contact the data exporter and, unlike the New EU SCCs, there is no requirement to contact the supervisory authority.

The Addendum is designed to be used alongside the New EU SCCs. It contains technical provisions that enable the New EU SCCs to work within the UK data protection regime.

IMPLEMENTATION

Organisations have been able to use the IDTA and Addendum since 21 March 2022, so new data transfer agreements entered into from that date should use the IDTA or New EU SSCs and Addendum to legitimise transfers. However, despite the IDTA and Addendum being in force, any agreements entered into on or before 21 September 2022, can still rely on the Old EU SCCs to legitimise data transfers until:

- 21 March 2024 for restricted data transfers **from the UK to jurisdictions outside of the EEA**; and
- 2 December 2022 for data transfers **from the EEA to third countries**.

For most organisations, use of the Addendum in conjunction with the New EU SCCs will be the preferred approach, as this will ensure compliance with the EU GDPR *and* UK GDPR, and will allow parties to change the scope of the data transfers without having to amend the transfer mechanisms in their existing agreements.

ICO RANSOMWARE GUIDANCE

SUMMARY

On 10 March 2022, the ICO published guidance on ransomware and data protection compliance (the "**Guidance**"). The Guidance was published after the ICO issued a monetary penalty to an organisation that was victim to a ransomware attack for failing to implement appropriate technical and organisational measures, and the National Cyber Security Centre ("**NCSC**") recognised ransomware as the biggest cyber security threat facing the UK. Jeremy Fleming, the director of GCHQ reported in October 2021 that the number of ransomware attacks on British institutions had doubled in 2021 compared to 2020.

USE OF THE GUIDANCE

The Guidance provides a summary of ransomware, why it is important as a data protection topic and what organisations can be doing to prevent it. It includes a checklist to be used by organisations when assessing general preparedness for ransomware attacks. The checklist covers points in relation to: (1) governance, (2) asset identification, (3) technical control selection, (4) access controls, (5) vulnerability management, (6) staff education and awareness, (7) detection, (8) incident response, (9) disaster recovery and (10) assurance.

In addition, the Guidance includes eight scenario-based examples that organisations can use to prepare for and respond to ransomware attacks, and mitigate the risk of such attacks. These are:

- **Scenario 1: Attacker sophistication.** The ICO stresses that ransomware attacks are not only targeted at large corporations and recommends that medium organisations assess their practices against the NCSC's "10 Steps to Cyber Security" guidance and certification under the ISO27001 Standard for Information Security Management;

- **Scenario 2: Personal data breach.** The ICO reminds data controllers that when they are subject to a cyber-attack, they have a responsibility and obligation to determine whether the incident has led to a personal data breach;
- **Scenario 3: Breach notification.** The ICO reminds organisations that data breaches should be notified to the ICO without undue delay and no later than 72 hours after the incident. The Guidance confirms that exfiltration, which occurs when malware and/or a malicious actor carries out an unauthorised data transfer from a computer, is an important factor to consider when conducting a risk assessment and determining if the breach should be notified to the ICO;
- **Scenario 4: Law enforcement.** The ICO reminds organisations that ransomware victims should contact law enforcements such as Action Fraud to notify them of the access to their data;
- **Scenario 5: Attacker tactics, techniques and procedures.** The ICO summarises the most common tactics, techniques and procedures that attackers use to gain access to systems and provides steps which organisations can take to mitigate these, such as: to provide training, undertake regular risk assessments, maintain proper documentation, implement appropriate measures in response to the risks, develop policies (e.g., access control policy), review permissions and utilise the NCSC vulnerability management guidance;
- **Scenario 6: Disaster recovery.** The ICO encourages organisations to backup any personal data that it processes and to ensure that its back-up procedures are suitable for the size of the organisation;
- **Scenario 7: Ransomware payment.** The ICO warns against the encouragement, endorsement or condoning of the payment of ransom, and against it being used as a means to restore any accessed personal data. This position brings the ICO in line with entities such as the U.S. government, which also strongly discourages all private companies from making ransomware payments; and
- **Scenario 8: Testing and assessing security controls.** The Guidance establishes methods of testing, assessing and evaluating an organisation's appropriate measures and recommends that organisations regularly test incident response plans, review user accounts and consider privileges, implement methods for checking vulnerabilities, perform regular audits of IT estates against a proven security standard and perform tests of the disaster recovery plan.

TAKE AWAYS

Whilst the Guidance is not legally binding, it is central in determining the ICO's approach when considering enforcement action against organisations who are victims of ransomware incidents. Organisations should therefore review the Guidance and take into account the recommendations and content when assessing and reviewing ransomware attack preparation and response plans. In addition, organisations should consider the ICO's position in relation to payment of ransoms (i.e. that such payments should not be condoned) and note that the position is not exclusive to the UK supervisory authorities, for example ransom payments are strongly discouraged by the UxS government.

FOR MORE INFORMATION

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

CLAUDIA SOUSA

+44 20 7903 1697
claudia.sousa@weil.com

WEIL.COM

#97864250

Weil