womblebonddickinson.com

WOMBLE BOND DICKINSON

Data Protection After Brexit

How will GDPR and UK GDPR affect US businesses?

March 23, 2021

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Introductions

Andrea T. Shandell
Vice President, Privacy Initiatives – Operations
BBB National Programs
ashandell@bbbnp.org

Tara Cho
Partner, Privacy and Cybersecurity
Womble Bond Dickinson (US) LLP
Tara Cho@wbd-us.com

Malcolm Dowden
Legal Director, Data Protection and Privacy
Womble Bond Dickinson (UK) LLP
Malcolm.Dowden@wbd-uk.com

Andrew Kimble
Partner, Data Protection and Privacy
Womble Bond Dickinson (UK) LLP
Andrew.Kimble@wbd-uk.com

Brexit, GDPR and UK GDPR

- 11.00pm 31 December 2020: Brexit implementation period ended.
- GDPR and UK GDPR are now separate legal regimes for personal data protection.
- US organisations operating across Europe now need to think about separate compliance procedures, and to be alert to any future divergence between the EU and UK.

Schrems II

- European Court ruling July 2020 invalidated EU-US “Privacy Shield”; and
- Confirmed SCCs as a *potentially* viable mechanism for transfers of personal data to non-EU/EEA countries, BUT
- Depending on the level of protection afforded by the receiving jurisdiction, SCCs might need to be accompanied by additional contractual or technical measures (e.g., strong pseudonymisation, encryption).

Standard Contractual Clauses

- Draft new SCCs issued by European Commission for consultation (consultation closed December 10, 2020)
- Key features of the new SCCs include:
  - Modular approach covering: (i) controller-to-controller; (ii) controller-to-processor; (iii) processor-to-processor; and (iv) processor-to-controller; and
  - “Docking clause” allowing a third party to join/accede to the SCCs at a later date

EU adoption of new Standard Contract Clauses

- Formal adoption requires an Opinion of the European Data Protection Board and a positive vote of EU member states through the comitology procedure.
- EDPB-EDPS joint opinion 19 January 2021 proposed several revisions to the consultation draft.
- EU Commission response and next steps to be confirmed.

EU adoption of new Standard Contract Clauses

- Proposed “grace period” of one year within which to implement the new SCCs for legacy transfers
- Trigger = new arrangements or variation to existing arrangements, so adoption might be required within the year’s grace period
- What does this mean in practice?

EU to UK transfers of personal data

- EU draft adequacy decision published February 2021.
- Likely to be adopted, but not yet a “done deal”.
- Conditional approval:
  - UK membership of the Council of Europe;
  - UK adherence to the European Convention of Human Rights and submission to the jurisdiction of the European Court of Human Rights;
  - UK adherence to the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”)

EU to UK and onward transfers

- “The level of protection afforded to personal data transferred from the EU to controllers or processors in the UK must not be undermined by the further transfer of such data to recipients in a third country”
- Such “onward transfers” should be permitted only where the further recipient outside the UK is itself subject to rules ensuring a similar level of protection to that guaranteed within the UK legal order”
- Potential for divergence? UK to begin making separate adequacy decisions from March 2021.

Separate EU and UK representatives

- GDPR and UK GDPR Article 27 each require the appointment of a representative where Article 3(2) (the “targeting test”) applies to overseas organisations.
- The “targeting test” applies when the overseas organisation does not have an “establishment” the EU or UK but where it offers goods or services or monitors the behaviour of data subjects in the EU and/or UK.
- Failure to appoint an Article 27 representative (where required) is a breach that under GDPR can result in a fine of up to €10 million or (if higher) 2% of global annual turnover.

Does the “targeting test” apply to your organisation?

- Offering goods or services, whether or not for payment
- What counts as monitoring behaviour?
- Does localised content/advertising count as targeting?

Profiling and automated decision-making

- GDPR and UK GDPR restrict profiling and solely automated decision-making, but protections are limited:
  - When are decisions made by “solely automated” means?
  - What are the consequences of challenge/objection?
  - How can algorithms be explained in a clear and comprehensible way?

Operating across regions

- GDPR-like personal data regimes are in place or forthcoming in a number of regions/jurisdictions, eg:
  - India
  - Nigeria (“NDPR”)
  - Kenya
  - South Africa
  - ADGM
  - DIFC
- Is a single, streamlined compliance regime possible?

Questions?

Appendix

- European Commission, draft adequacy decision: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661

- UK Department for Digital, Culture, Media and Sport (DCMS), National Data Strategy: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

Appendix

- European Data Protection Board (EDPB) Recommendations on supplementary measures following *Schrems II*: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

- EDPB Statement on the end of the Brexit implementation period: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-end-brexit-transition-period-update-13012021_en

- EDPB and European Data Protection Supervisor joint Opinion on new Standard Contract Clauses: https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en

Appendix

- UK Information Commissioner's Office (ICO) guidance on data protection after Brexit: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/
- ICO statement on EDPB Schrems II recommendations: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/updated-ico-statement-on-recommendations-published-by-the-european-data-protection-board-following-the-schrems-ii-case/
- Law Society of England and Wales guidance on data flows after Brexit: https://www.lawsociety.org.uk/en/topics/brexit/end-of-transition-period-guidance-eu-data-flows
- ICO enforcement actions: https://ico.org.uk/action-weve-taken/enforcement/

Appendix

- EDPB Guidelines on the territorial scope of GDPR: https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en

- ICO guidance on European Representatives: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/european-representatives/

- ICO guidance on UK Representatives: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/uk-representatives/

Appendix

- FBI – Internet Crime Complaint Center Public Service Announcement about online scams: https://www.ic3.gov/media/2020/200420.aspx
- FBI Alert Re: COVID-19 phishing attack targeting healthcare providers: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436494/COVID_Phishing_FLASH_4.20_FINAL.pdf
- National Security Agency guidance on selection and secure use of telecommuting tools: https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF

Appendix

- Health Sector Cybersecurity Coordination Center white paper on exploitation of videoconferencing services: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436539/TLPWHITE_UNCLASSIFIED_20200402-COVID-19%20VTC%20Exploitation%20%28002%29.pdf

- Health Sector Cybersecurity Coordination Center brief on COVID-19 related cyber threats: https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436438/TLP_WHITE_UNCLASSIFIED_20200423-COVID-19_Cyber_Threats.pdf

- U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) alert on COVID-19 related cyber attacks: https://www.us-cert.gov/ncas/alerts/aa20-099a