Bird & Bird & New EDPB Guidelines, New SCCs … Too much on my plate!

60 minutes to digest it all!

Ariane Mole
Partner, France
ariane.mole@twobirds.com

Fabian Niemann
Partner, Germany
fabian.niemann@twobirds.com

James Mullock
Partner, UK
james.mullock@twobirds.com

Schrems II

- Privacy Shield invalid
- SCCs still valid, BUT…

transfer tools must be "effective" and a level of protection essentially equivalent to that offered within the E.U must be guaranteed.

<u>Since then</u> :

Open to public consultation

- Draft Guidance on Additional Measures to Supplement SCCs (EDPB)
- Draft New SCCs (E.C.)
- Draft New Standard Processor Clauses under Article 28 GDPR (E.C.)

Bird & Bird

Bird & Bird & New EDPB's Guidance on Supplementary Measures

Draft Recommendations

(November 10, 2020 – Open to public consultation until December 21)

Scope

- All data exporters in the EU : either Controller or Processor
- Not only SCCs : All GDPR Article 46 tools, including BCRs
- All transfers : includes remote access from a third country, cloud infrastructure (unless EU based only) and onward transfers

CARRY OUT A DATA TRANSFER ASSESSMENT : 6 STEPS OF HARD WORK	
1. Know your transfers	Map destinations – Know where data is processed. Should be done already according to GDPR but difficult to check all onward transfers and chain of subprocessors
2. Identify your transfer tools	- Adequacy - Article 46 tools : SCCs, BCRs Derogations (consent, etc). Must remain exceptional.
3. Assess effectivity of Article 46 tools	Toughest Step : - In the light of all circumstances of the transfer (purpose, entities involved and type of recipients, data transferred, onward transfers…) - Assess effectivity of the tool based on publicly available legislation of the third country, with the help of the importer (§30)= if public authority access is proportionate and if data subjects are provided with effective redress - NB : Such assessment was done already for the US by the CJUE
4. Adopt Supplementary measures	To fill the gap if assessment under Step 3 reveals that transfer tool is not effective
5. Procedural step	Put in place transfer tool if Step 3 or Step 4 allows for effectiveness / appropriate guarantees If not, do not transfer
6. Re-evaluate regularly	*"Accountability is a continuing obligation (art.5 (2) GDPR"*

rd

No leniency (even if requirements laid down by Schrems II are hard to meet)

§42 : "*Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likehood of public authorities access to your data in a manner not in line with E.U. standards. You should conduct this assessment with due diligence and document it thoroughly, as you will be held accountable to the decision you may take on that basis.*"

Bird & Bird

What are Supplementary Measures?

Technical, Contractual, Organisational

I. Technical Measures : very few possibilities, conditions for effectiveness are very strict

- **Encryption**, under conditions that :
  - ✓ Keys are retained solely under the control of the data exporter in the EEA or adequate country → Applicable for back-up purposes if the processor in third country does not need access to data
  - ✓ Or professional secrecy of the importer prohibits surveillance authorities from accessing to data

- **Pseudonymisation** under conditions that :
  - ✓ Data cannot be attributed to specific individual nor be used to single out the individual in a larger group, without the use of additional information held only by the exporter in the EEA or adequate country
  - ✓ The exporter has established that the public authorities of the third country cannot cross the pseudonymised data with other information for re-identification

- **Split of buckets of data between several processors**, each in a different country, without disclosing identifiable data to either of them

Bird & Bird

Other examples of scenarios with technical measures are found ineffective by the EDPB to legitimise the transfers, such as :

- Transfers to a cloud services provider where data is needed in clear text by the processor for it to carry out its task
- Transfers for shared business purposes, for ex. of employee data by an EU subsidiary to its mother company in the US
- Where data is encrypted, but cryptographic keys are not held only by the EU exporter, so that surveillance authorities in the third country can access to the keys (as in the case under FISA 702 in the US)

Bird & Bird

II. Contractual Measures :

Some of the recommended contractual measures are part of the obligations of the importer in the new SCCs:

- Inform exporter and data subjects that there is a request from an authority
- Challenge the request and minimize data provided
- Assist data subjects in exercising their rights through redress mechanisms
- No back doors
- Provide "warrant canary"
- Restrictions on onward transfers

III. Organisational Measures :

- Internal policies on operating procedures in case of requests
- Internal record on requests received, available to exporter and data subjects
- Regular publication of transparency reports

NB : Contractual or Organisational Measures are not sufficient without effective Technical Measures, since they cannot bind public authorities in the third country. They can only complement the Technical Measures.

Bird & Bird

Microsoft first to announce measures …

New Steps to Defend Your Data

Nov 19, 2020 | Julie Brill - Corporate Vice President for Global Privacy and Regulatory Affairs and Chief Privacy Officer

Defending Your Data makes a substantial addition to our foundational privacy promises, and builds on the strong protections we already offer customers.

- **We use strong encryption:** We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
- **We stand up for customer rights:** We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
- **We are transparent**: We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we disclose more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular Law Enforcement Request Report.
- **We have a track record of legal success.** We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.

Bird & Bird

… immediately criticized by NOYB

SOURCE: NYOB

- First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.
- Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.

We call these protections Defending Your Data, and we will begin adding them to our contracts with public sector and enterprise customers immediately.

Defending Your Data makes a substantial addition to our foundational privacy promises, and builds on the strong protections we already offer customers.

- **We use strong encryption:** We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
- **We stand up for customer rights:** We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
- **We are transparent**: We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we disclose more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular Law Enforcement Request Report.
- **We have a track record of legal success.** We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.

Duty under Article 6(1)(c) – if there is no duty to comply (illegal request) then you can't provide the data… Challinging it is the logical consquence - nothing new…

Duty under Article 82 GDPR, but without all the limits (no class action, burden of proof on the user, etc) that Microsoft put into it's contract and that would actually limit (!) data subejcts' (third party) rights!

Required under Article 32 GDPR - big News.

Yeah, so Microsoft complies with FISA 702 which is the „legal process".

Yeah, so you even disclose that you provided the data of 28.500 to 29.998 accounts in 2019.

Congrats, good job on SCA – but frankly overturend by the Cloud Act and irrelevant when this is about FISA 702.

Bird & Bird

Different reactions depending on Member-States

- **Germany:** Microsoft initiative was well received by the DP Authorities of Baden-Wurttemberg, Bavaria, and Hesse
- **France :**
  - French DPA (CNIL) said in October 2020 that supplementary measures are unlikely to be effective if taken by an electronic communication service provider which is submitted to requests from US surveillance authorities;
  - Concerning the Health Data Hub, French Supreme Court (Conseil d'Etat) ruled that there are risks even where data is hosted in the E.U. and even where data is pseudonymized, if the hosting provider is a US company (submitted to US law)

- **NOYB complaints** : few DPAs have started investigations, it seems that others (the majority) have not

Bird & Bird

Where do we stand now ?

- The EDPB guidance gives no comfort (for most transfers)
- Use the public consultation period to send comments to the EDPB (for example on §42);
- Document Data Transfer Assessments : Follow the recommended Steps
- Put in place all possible supplementary measures
- Adopt a risk based approach
- Watch if and how enforcement practice develops

Bird & Bird

Bird & Bird & New SCCs

Draft Implementing Decision on new EU standard contractual clauses for the transfer of personal data to third countries

(November 12, 2020 – Open to consultation until December 10 2020)

High level summary

1. Background and structure
2. What is covered
3. Some key issues – US transfers, supplemental terms, liability
4. Summary – The Good, the Bad and the Ugly

Bird & Bird

Background and structure

- On 12 November 2020, the European Commission published a draft Implementing Decision on new standard contractual clauses for the transfer of personal data to third countries ("**Clauses**"), consisting of (i) the decision with reasoning, and (ii) the actual Clauses

- Goals
  - Trying to reflect **Schrems II**
  - Addressing **known deficiencies** in current SCCs such as catering for data transfers by EU processors to sub-processors and from EU processors back to their instructing controller

Background and structure

- Difficult topic and Commission has introduced significant improvements to the current SCCs, but some issues remain and there are also some new issues
- Significant job for parties to **move to the new Clauses**
  - resign agreements
  - provide enhanced transparency to data subjects
  - flow down new terms to third parties and sub-processors
  - only a **one year transition period** for this to be done
- The Clauses are open for **consultation until 10th December 2020**

Background and structure

- **Modular approach**, covering (i) C2C, (ii) C2P, (iii) P2SP, and (iv) P2C
- Allowing **multiple parties** to join (and accede later)
- Section 1: Purpose and scope
  - applicable to all
- Section 2: Obligations of the parties
  - Modular, i.e. different clauses for different scenarios with some clauses applying to all or to a number of scenarios
- Section 3: Final provisions
- Annexes: (i) parties & transfer descriptions, (ii) TOMs, (iii) sub-processors

What is covered?

Addressing Schrems II:

- Keeping existing mechanism which were the reason for the CJEU to say that existing SCCs remain valid, i.e. obligations of
  - exporter (assisted by importer) to consider level of protection of personal data in the third country
  - importer to notify exporter of any inability to comply with SCCs
  - exporter to suspend data transfers, terminate the agreement, or to notify the supervisory authority in such case

What is covered?

Addressing Schrems II:

- Additional safeguards:
  - Exporter to undertake & document a **transfer impact assessment** (to be made available to the competent authority on request); Clauses set out factors to be considered in the assessment
  - **In addition to considering the law and practice in the third country**, the draft Clauses also **helpfully reference** i.a. the duration of the contract; scale and regularity of transfers; length of processing chain and transmission channel used; type of recipient; purpose of the transfer and the nature of the data transferred **(does this allow some flexibility?)**

What is covered?

Addressing Schrems II:

- Additional safeguards:
  - **stronger commitments** of importer vis a vis third country authorities: (i) where possible **notify both** exporter and data subject; (ii) assess legality of request and, where it considers it has grounds to **challenge** the order, it must do so; (iii) where possible seek an **interim measure** to suspend disclosure; (iv) in any case only disclose **minimum** possible; (v) **document** all and make available to exporter
- EDPB recommendations addressed, but not all of them

What is covered?

New: some **GDPR-like obligations** of the importer under the Clauses:

- **Increased and (onerous) transparency** obligations (in particular in C2C); clear and plain language, as in Art.12 GDPR
- Some **data subject rights** (access, erasure and rights to object to processing for direct marketing) are also included
- But **no complete shift** of GDPR on importer, e.g. the burdensome provisions relating to records of processing activity and data protection impact assessments are not included

Onward transfers stricter, e.g. C2C module requires third party recipient of transfer from importer to accede SCCs

Some key issues

Supplemental terms

- There is often uncertainty as to what extent parties can introduce supplemental terms without violating the prohibition on contradicting provisions in the SCCs.
- The Commission has tried to make clear that additional clauses can be used, so long as they do not contradict the Clauses or undermine protections for individuals. However, **what does this actually say?**
- It would be helpful if the Commission could do more to **reduce the uncertainty and expressly allow flexibility** where possible; by more optional clauses and by making clear that clauses which are concerned with process, rather than substance, do not contradict the Clauses. Ideally they list expressly what is mandatory and what is not.

Some key issues

Liability

- Other than eg the 2001 C2C and the 2010 C2P (and like the 2004 C2C) SCCs, the Clauses include express **rules on liability between Exporter and Importer**
  - For material and **non material** breaches of the Clauses
  - Liability (only) limited to **actual damage**; no punitive damages
  - Indemnification for damages caused by responsibility of the other (eg data subject claims)
- **Deviations possible?**
  - Decision says "*standard contractual clauses should provide for rules on liability between the parties and with respect to data subjects, as well as rules on indemnification between the parties*"
  - Any rules or the suggested rules?

Some key issues

Transfers to countries with no adequate laws in view of the EU (e.g. US): is there a flexibility to consider the circumstances of the individual case?

- 19) of the decision is **strict, referring just to the laws in abstract**: "*The transfer and processing of personal data under standard contractual clauses should only take place if the laws of the third country of destination do not prevent the data importer from complying with those clauses*."

Some key issues

Transfers to countries with no adequate laws in view of the EU (e.g. US): is there a flexibility to consider the circumstances of the individual case?

- 20) of the decision (and the Clauses themselves) provides more **flexibility, allowing considering the individual circumstances**: "*To that end, they should in particular take into account the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data transferred, the type of recipient, the purpose of the processing and any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred), ...*" [the laws of the third country, TOMs]

Summary

Good	Bad	Ugly
Modular approach	Lack of clarity re supplemental rules	Long Arm (onward transfers)
Covering multiple scenarios and parties	Lack of clarity re liability	GDPR-like obligations extended
Extension of scope to P2SP and P2C	Lack of clarity re US transfers (though this is rather caused by CJEU)	Heavy Schrems II related obligations (caused by CJEU)
Trying to address Schrems II somehow pragmatic	Heavy documentation requirements	1 year grace period only

Bird & Bird

Want to know more?

Check out our article:

European Commission publishes proposed replacement Standard Contractual Clauses

Bird & Bird

Bird & Bird & New EC A28 SCCs

Draft proposal

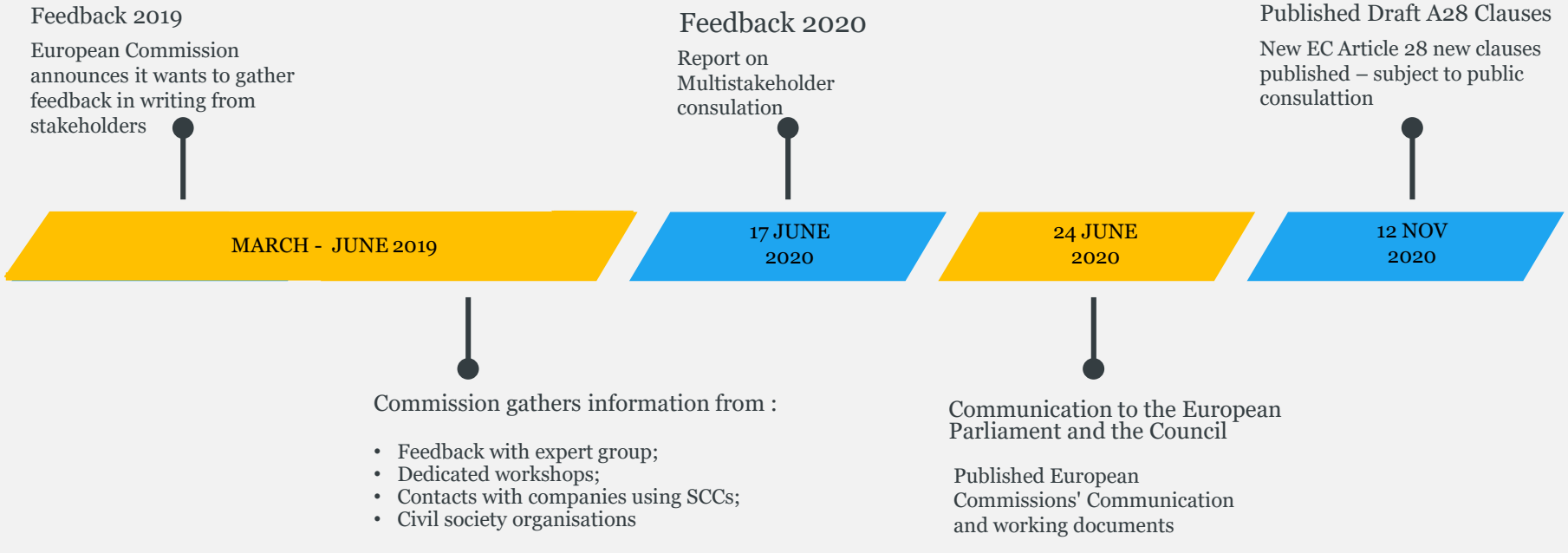
(November 12, 2020 – Open to consultation until December 10 2020)

High level summary

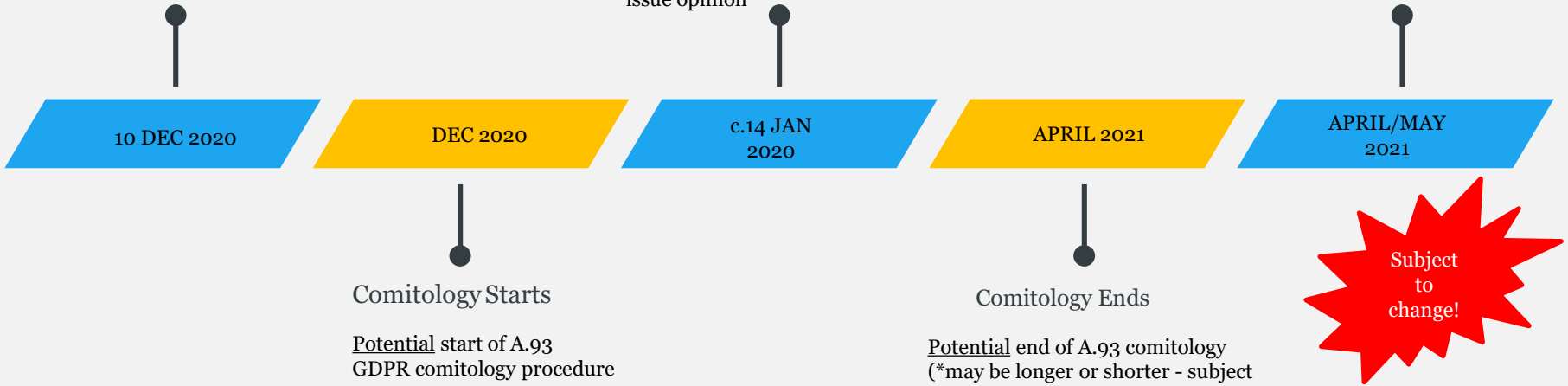
1. What: The EC's draft C2P A28 clauses published 12 Nov
2. Why: GDPR A28(7)
3. When: Unlikely to be finalised before Q2 2021
4. Where can I find them? Click here
5. Are they any good?

Bird & Bird

Timeframe: EC's draft C2P A28 SCCs (1)



Timeframe: EC's draft C2P A28 SCCs (2)



Some introductory comments

1. They are presented as an annex. Presumably they are intended for use as a schedule to an MSA
2. They themselves have 7 annexes – e.g. processing purposes, sub-processor lists, x3 TOMs!
    - Note: the security TOMs gold plate the GDPR by referring to transfer SCC requirements, e.g. protection during transmission
3. No modification permitted but additions ok (provided they don't contradict the core SCCs)
4. They take precedence over any agreement made between parties. What about transfer SCCs, which takes precedence?

Bird & Bird

Review: the good

1. Modular approach
2. Multiple parties – docking clause allows easy addition of a new party [but note point 1 on my final slide]
3. Potential to interlink with transfer SCCs
4. Some options within clauses – e.g. use of sub-processors
    - Although approach is unsophisticated

Bird & Bird

Review: the bad

1. (Bad for DP) – limited reference to DC covering costs
   - Would have to be included in MSA
2. (Bade for DC) – breach notification by DP:
   - Longstop deadline = 48 hours. No reference to suspected breaches
3. Inconsistencies with EDPB Controller/Processor guidance
   - E.g. DP obligation to inform DC if instructions infringe GDPR – guidance requires details of 'consequences' of infringement
4. Appears to be no ability for DC to change its mind about whether data should be returned or erased on termination
   - Even the EDPB guidance supports this

Bird & Bird

Review: the ugly

1. Inconsistencies with the transfer SCCs
    - E.g. DP support & audit provisions in transfer SCCs permit DC to consider 'relevant certifications' in place of audit but A28 SCC don't
2. Sub-processor appointment approval clauses don't deal with scenario where DC withholds consent
3. x3 inconsistent breach notification clauses
4. Requirement to identify competent DPA for security breach notifications
5. Requirement for DPA to have access to audit reports

Bird & Bird

Finally: some MSA drafting points

1. If the SCCs are used as a schedule to an MSA care needed as to how entities which are not parties to the MSA are added to take the benefit of the SCC, e.g. group cos
    - The SCCs assume that the docking clause will be used. That many not work in the context of the MSA
2. No liability provisions in SCCs
3. Care needed when adding SCCs as a schedule to an MSA
    - E.g. Non-personal data security & certification commitments will be needed in addition to Annex III

Bird & Bird

Check out our articles:

European Commission publishes proposed replacement Standard Contractual Clauses

EDPB Publishes draft recommendations on data transfer post Schrems II - path forward for many transfers remains uncertain

New EDPB FAQs on Schrems II: what are the main takeaways?

Schrems II judgment: Privacy Shield invalid, SCCs survive, but… what happens now?

Thank you & Bird & Bird

And don't forget to follow us on LinkedIn: @Bird & Bird Privacy & Data Protection

twobirds.com