PROGRAM MATERIALS
Program #2943
March 6, 2019

"I'm the controller!" "No, I am!": Joint Controllers under the GDPR

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

“I’m the Controller!” “No, I am!”

Joint and Separate Controllers Under The GDPR

Sean Christy & Tyler Thompson

BRYAN CAVE LEIGHTON PAISNER BCLP

Goals of This Presentation

Understand

- Understand how to identify if a relationship between multiple parties is controller-processor, separate controllers, or joint controllers
  - Understand the implications of each type

Learn

- Learn key considerations in structuring and papering joint controller relationships

Practice and discuss

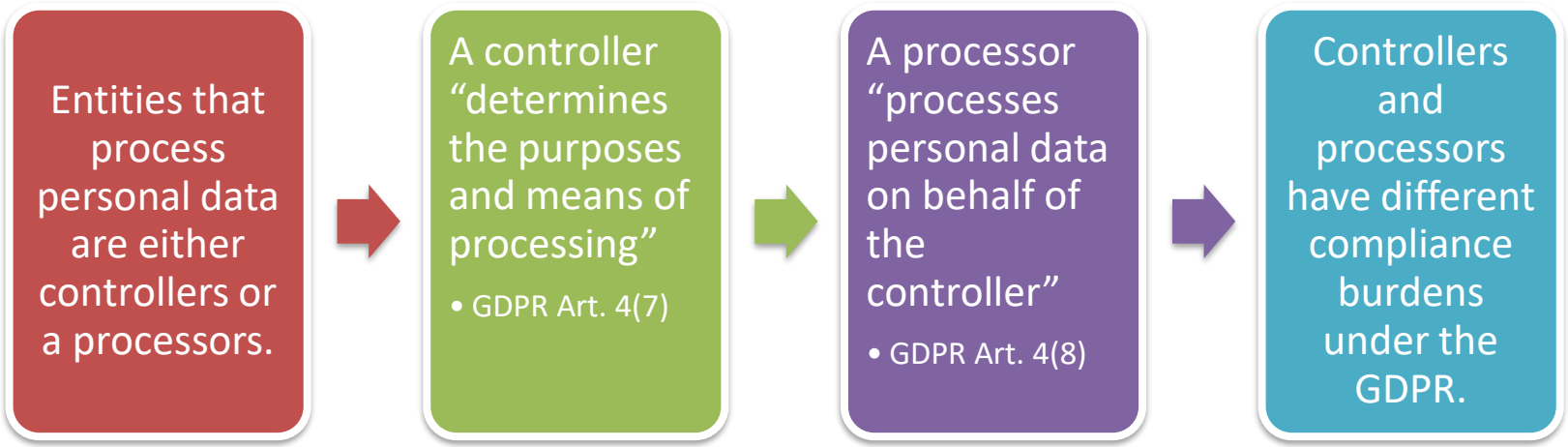
- Practice and discuss with real scenarios

BRYAN CAVE LEIGHTON PAISNER BCLP

Determining The Relationship Between Parties

BRYAN CAVE LEIGHTON PAISNER BCLP

GDPR Controllers and Processors



BRYAN CAVE LEIGHTON PAISNER BCLP

Joint and Separate Controllers

- Controllers may be a separate, stand-alone controller that is entirely responsible for compliance with controller GDPR obligations.
  - Exactly as if they were the sole controller of the personal data.

OR

- Two *or more* Controllers may be **joint controllers**, and allocate the controller responsibilities between them.

- Joint Controllers permitted in GDPR Art. 26:
  - "[Joint controllers] shall determine their respective responsibilities for compliance with the obligations under this Regulation… by means of an arrangement between them…"

- "Joint control will arise when different parties determine… either the purpose or those essential elements of the means which characterize a controller"
  - WP 169 at 19

- "The fact that different entities cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases."
  - WP 169 at 19

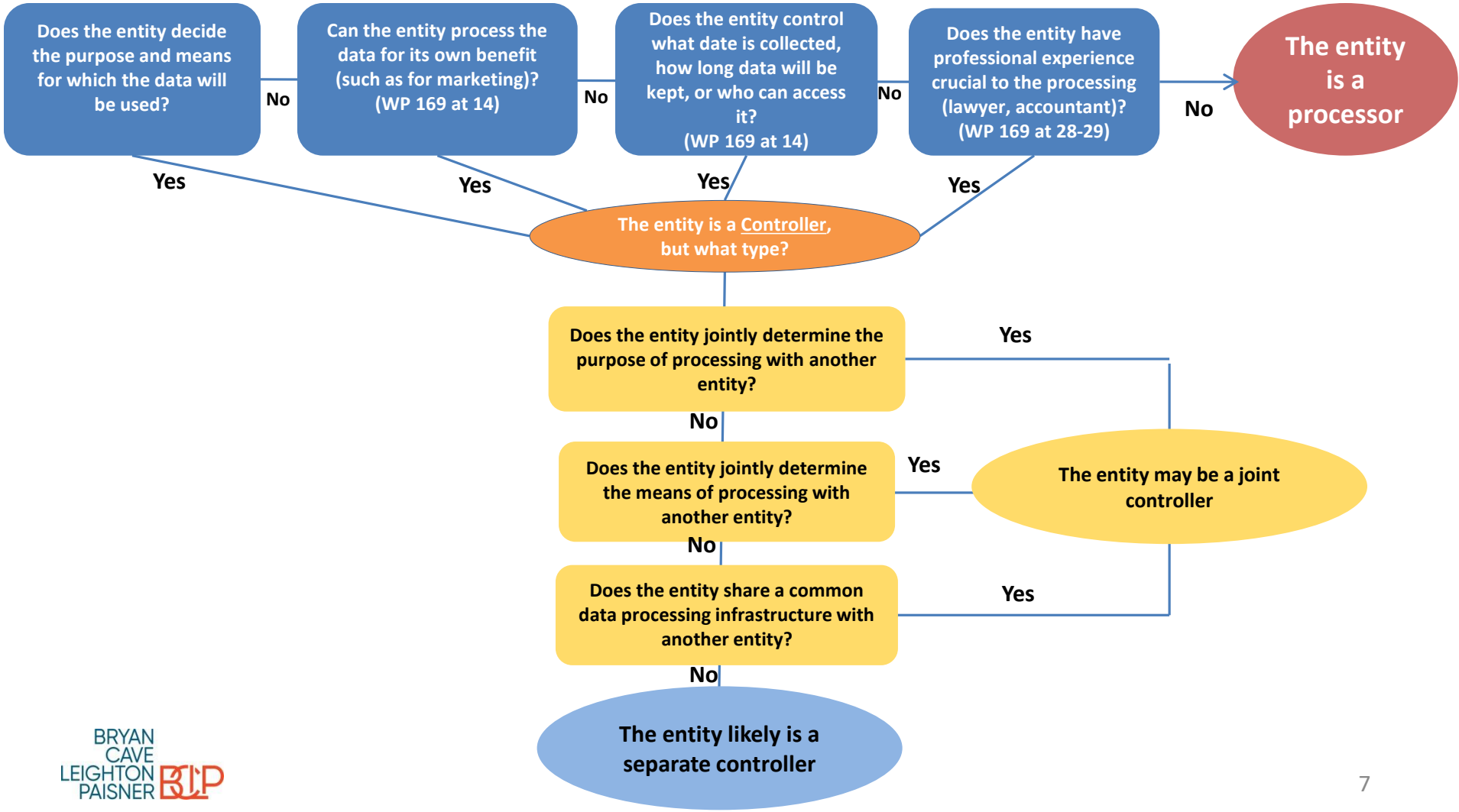
BRYAN CAVE LEIGHTON PAISNER BCLP

Determining Processor, Separate Controller, Joint Controller

- This determination is usually a factual determination
  - EU regulator will ignore how the parties have positioned themselves via contract
    - "Contractual agreements can be useful in assessing joint control, but should always be checked against the factual circumstances of the relationship between the parties."
      - WP 169 at 18
    - Remember this when we talk about advantages and disadvantages
  - It's possible law requires a certain party be a controller
    - Not factual in this case

BRYAN CAVE LEIGHTON PAISNER BCLP

Determining Processor, Separate Controller, Joint Controller (Cont'd.)



BRYAN CAVE LEIGHTON PAISNER BCLP

Agreements Between Processors, Separate Controllers, Joint Controllers

Processors:	Separate Controllers:	Joint Controllers:
GDPR Article 28 Data Protection Agreements	No contractual agreement needed ***BUT*:**	a Joint Controller agreement
Must contain all the provisions of GDPR Art. 28 These are the most common and are generally seen as well understood and settled.	Can the disclosing controller: • Share without violating their privacy policy? • Provide a permissible purpose for sharing? Can the receiving controller: • Provide a permissible purpose for its processing? • Provide the data subject with transparency (i.e. a privacy policy)? • Is there a cross border transfer that requires standard contractual clauses?	Can be with more than two parties Participation of the parties does not need to be equally shared • WP 169 at 19 Less standardized and settled than a GDPR Art. 28 agreement No "requirements" listed in the GDPR

BRYAN CAVE LEIGHTON PAISNER BCLP

Advantages and Disadvantages

Controller-Processor GDPR Art. 28		Joint Controllers GDPR Art. 26		Separate Controllers	
PRO	**CON**	**PRO**	**CON**	**PRO**	**CON**
Common and Familiar	Processor data use is extremely restricted	Allows for both parties to use data in a variety of ways	Requires a high degree of coordination between controllers	Each party remains fully responsible for its own obligations	Data subjects may not expect this type of sharing
Controller has complete control	Easy to stray outside of the boundaries placed on processor	Controllers can present one privacy policy, data subject point of contact.	Difficult to paper by comparison		Difficult to establish a permissible purpose to share, provide privacy policy

Joint Controller Agreements

BRYAN CAVE LEIGHTON PAISNER BCLP

What is a Joint Controller Agreement?

- "[Joint controllers] shall determine their respective responsibilities for compliance with the obligations under this Regulation… by means of an arrangement between them…"
  - GDPR Art. 26(1)
- The arrangement… shall duly reflect the roles and relationships of the joint controllers vis-à-vis the data subjects
  - GDPR Art. 26(2)
- "The bottom line should be ensuring that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights… are not ensured by any of the parties."
  - WP 169 at 22
- What if joint controllers don't have an agreement?
  - No guidance
  - Possibly joint and several liability for all controller obligations.

BRYAN CAVE LEIGHTON PAISNER BCLP

Joint Controller Agreement Provisions

- We suggest a chart that allocates each responsibility to one controller or the other (shown on next slide).

3.1 **Allocation of Compliance Obligations.** The Parties agree to allocate compliance obligations for the Data Protection Laws as described in the following table. If a single controller is listed as responsible for a compliance obligation, that controller shall be solely and exclusively responsible and liable for the compliance of both controllers for the obligation noted. If multiple controllers are listed as responsible for a compliance obligation, or if no controller is listed as responsible for a compliance obligation, each controller shall be responsible and liable for their own compliance obligations, and shall not be responsible or liable for the compliance of the other controller.

- Non-responsible controller has duty of cooperation.

3.4 **Reasonable Cooperation of Non-Responsible Controller.** A party that is not responsible for a compliance obligation, or a party that is jointly responsible for a compliance obligation, shall reasonably cooperate with the Responsible Controller as necessary to fulfil the Responsible Controller's obligations.

- ***BCLP's Joint Controller Agreement template is available upon request***

BRYAN CAVE LEIGHTON PAISNER BCLP

Joint Controller Agreement Provisions

Compliance Obligation[1]	Controller A	Controller B
Lawful Purpose. Validating the sufficiency of the lawful basis upon which processing is based in compliance with GDPR, Article 6, Article 7, and Article 9 (*e.g.*, documenting consent if consent is the lawful basis for processing).	Choose an item.	Choose an item.
Privacy Notices. Providing data subjects with an accurate privacy notice, if required, pursuant to GDPR, Articles 13 and/or 14 and endeavouring to make the nature of this joint controller relationship available to the data subjects pursuant to GDPR Article 26(2).	*Controller A will provide privacy notice.*	*Not responsible.*
Data Subject Access Requests. Respond to requests from data subjects for access to their Personal Data, pursuant to GDPR, Article 15 and/or 20.	*Select from drop down*	*Select from drop down*
Data Subject Rectification Requests. Respond to requests from data subjects to correct their Personal Data, pursuant to GDPR, Article 16.	*Select from drop down*	*Select from drop down*
Data Subject Erasure Requests. Respond to requests from data subjects to erase their Personal Data, pursuant to GDPR, Article 17.	*Select from drop down*	*Select from drop down*
Data Protection Officer. To the extent one is required, appoint a Data Protection Officer pursuant to GDPR, Article 37.	*Select from the drop down*	*Select from the drop down*
EU Representative. To the extent one is required, appoint a representative within the Europe Union pursuant to GDPR, Article 27.	*Select from the drop down*	*Select from the drop down*
Data Protection Impact Assessment. To the extent one is required, conduct a data protection impact assessment pursuant to GDPR, Article 35.	*Select from the drop down*	*Select from the drop down*
Contacting Regulators In the Event of a Security Breach. To the extent required, contacting regulators to notify them of a security breach pursuant to GDPR, Article 33.	*Select from the drop down*	*Select from the drop down*
Contacting Data Subjects In the Event of a Security Breach. To the extent required, contacting data subjects to notify them of a security breach pursuant	*Select from the drop down*	*Select from the drop down*

BRYAN CAVE LEIGHTON PAISNER BCLP

Lawful Purpose of Processing

- Under Art. 6, processing is only lawful if there is a lawful purpose of processing
- Which controller will evidence permissible purpose?
  - Consent
    - Which controller is responsible for ensuring consent is properly collected and can be evidenced?
  - Performance of Contract
    - Which controller has entered into the contract and can evidence its execution? Does the contract make clear that the processing is necessary for performance?
  - Legitimate interest
    - Which controller has articulated the legitimate interest and undertaken the balancing test to ensure such interest isn't overridden by the fundamental rights and freedoms of data subjects?

BRYAN CAVE LEIGHTON PAISNER BCLP

Privacy Notice/Policy

"The essence of the arrangement shall be made available to the data subject."

GDPR Art. 26(2)	Adds another requirement to the privacy notice disclosures of GDPR Art. 13-14

Providing a single privacy notice is one of the *biggest advantages* of a joint controller relationship.

Crucial that the controller *not* providing the notice be obligated to provide all necessary information to the providing controller.

BRYAN CAVE LEIGHTON PAISNER BCLP

Data Subject Requests

- Articles 15-21 give data subjects a variety of rights which they can exercise against controllers upon request.
- "The [joint controller agreement] may designate a contact point for data subjects."
  - GDPR Art. 26(1)
- The agreement should designate which party responds and obligate them to:
  - Respond within GDPR timeframes
  - Verify identity of the requestor
  - Be liable for refusal to respond

3.3 **Data Subject Requests.** The Controller responsible for Data Subject Access Requests, Data Subject Rectification Requests, or Data Subject Erasure Requests, as set forth in Section 3.1 above, may request that the non-responsible Controller take certain actions with Personal Data under its control in order to comply with these requests. The non-responsible Controller shall either 1) promptly take such actions and certify their completion in writing to the responsible Controller, or 2) provide the other controller with a written explanation to the data subject of why such action is not required by the Data Protect Laws and become exclusively liable for its refusal to comply.

BRYAN CAVE LEIGHTON PAISNER

Data Protection Officers

- DPO: GDPR Art. 37
  - Broadly, DPOs are required when the controllers core activities consist of large scale processing of special category data or regularly monitor data subjects
- A single DPO can arguably be appointed for the joint processing of both controllers.
  - "A group of undertakings may appoint a single data protection officer…"
    - GDPR Art. 37(2)
  - But, what about attorney-client privilege?
- Each controller having a DPO presents issues as well
  - How do you handle when the DPOs' advice conflicts?

BRYAN CAVE LEIGHTON PAISNER BCLP

Data Protection Impact Assesment

- DPIAs assess the impact of processing on the protection of personal data in high risk scenarios.
  - GDPR Art. 35
- Which controller will be responsible for the DPIA?
  - Prior consultation with supervisory authority in the event of a “high risk” assessment.
    - GDPR Art. 36(1)

BRYAN CAVE LEIGHTON PAISNER BCLP

Personal Data Breach

- GDPR Article 33 & 34 deal with Personal Data Breaches
- There is no breach notification timeline between joint controllers.
- Considerations in a Joint Controller Agreement:
  - Require notification of the other controller
  - Decide which controller will conduct the risk assessment, and if the other controller has any recourse if they disagree with the assessment
  - Decide who will contract regulators and data subjects

Contacting Regulators In the Event of a Security Breach. To the extent required, contacting regulators to notify them of a security breach pursuant to GDPR, Article 33.	*Controller A is not responsible for notifying regulators, but must notify Controller B immediately upon becoming aware of a security breach.*	*Controller B shall be responsible for notifying regulators and shall provide Controller A with a copy of such notification.*

BRYAN CAVE LEIGHTON PAISNER

Data Inventory

- "Records of processing" required by Art. 30.
- Can joint controllers have a single inventory for processing? Or does each controller need an inventory?
  - Art. 30(1): "*Each controller*… shall maintain a record of processing activities"
- The record must include the name and contact details of the joint controller
  - Art. 30(1)(a)

Compliance Obligation[1]	Controller A	Controller B
Data Inventory. Maintaining a record of processing activities (*e.g.*, data inventory) in compliance with GDPR, Article 33.	*Controller A is not required to maintain a record of processing activities, but shall provide Controller B all information needed to keep its record current.*	*Controller B will maintain a record of processing activities.*

BRYAN CAVE LEIGHTON PAISNER

Indemnification, Limitation of Liability

- Indemnification for the other controllers breach of the GDPR or failure of a compliance obligation allocated to them should be standard.
- BCLP best practice is to disclaim consequential damages
  - Consequential damages of breaches can be extremely high
- Except for disclaiming certain damages types, unlimited liability should be the goal in most arrangements
  - Failure of one controller to correctly undertake the compliance obligations for the joint controllers could expose all controllers to GDPR liability
- Be wary of making these damages subject to the cap of the master agreement…
  - Example: Controller 1 is a United States company with no establishment in the EU. Controller 1 is responsible for collecting data subject consent for processing under the joint controller agreement but has not done so. An EU supervisory authority assesses a penalty for this violation. The other joint controller, Controller 2, is established in the EU. The supervisory authority decides to enforce the penalty against Controller 2 to avoid dealing with extraterritoriality enforcement issues. Damages for breach of the joint controller agreement are subject to the MSA limitation of liability between the parties, which caps all damages except for IP infringement to the fees paid under the MSA.

BRYAN CAVE LEIGHTON PAISNER BCLP

Data Transfer and Onward Processing

- GDPR cross-border transfer rules still apply to joint controller arrangements.
  - Ensure that the joint controllers have a valid way to transfer data out of the EU if necessary
- Between joint controllers and processors other controllers
  - Make the joint controller engaging the processor fully liable for the processor

Onward Transfers[2]	Controller A	Controller B
To controllers that are not a party to this agreement.	*Controller A may not provide Personal Data to a Controller that is not a party to this Agreement, unless that Controller is under common ownership or controller with Controller A.*	*Controller B may not provide Personal Data to a Controller that is not a party to this Agreement, without Controller A's consent.*
To processors.	*Controller A may provide Personal Data to a processor that is approved, in advance, by Controller B.*	*Controller B may provide Personal Data to a processor if Controller A is notififed in advance as to the processor and provided an opportunity to object.*

BRYAN CAVE LEIGHTON PAISNER

Other Provisions

3.2 **Recovery of Costs for Compliance.** The parties agree that between themselves the costs and expenses incurred by a Controller in the fulfilment of the compliance obligations identified within Section 2.1 will be allocated as follows: *Option 1: Each Controller shall bear their own costs for compliance.*

4.1 **Data Minimization.** The Parties shall keep Personal Data under their control in a form that permits identification of Data Subjects for no longer than is necessary for the purpose for which the data was Processed.

4.2 **Access to Compliance Documents**. Each Party shall make records relating to compliance available to the other Party, or any third party with a right to view such records, upon request.

4.3 **Confidentiality**. Each Party shall take reasonable steps to ensure the reliability and confidentiality of any employee, agent or contractor who may have access to the Personal Data, ensuring that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with applicable law.

Audit Rights. Each Party shall be entitled to verify, either personally or by means of an independent third party bound by sufficient confidentiality obligations that the other Party is acting in compliance with this Agreement and the Data Protection Laws (an "**Audit**"). As part of an Audit, the audited Party shall provide the other Party with all information reasonably required to carry out such Audit. Audits may occur no more than once per calendar year and shall be conducted at audited Party's place of business at a time reasonably acceptable to the Audited Party. The auditing Party must notify the Audited party of its intent to Audit at least fifteen business days prior to conducting the Audit. The Auditing Party shall use best efforts to minimize the use of the audited Party's personnel time and disruption to the audited Party's business.

BRYAN CAVE LEIGHTON PAISNER LLP

Examples and Discussion

BRYAN CAVE LEIGHTON PAISNER BCLP

Headhunter

- Company Headhunterz Ltd helps Enterprize Inc in recruiting new staff. The contract clearly states that "Headhunterz Ltd will act on behalf of Enterprize and in processing personal data acts as a data processor. Enterprize is the sole data controller". However, Headhunterz Ltd is in an ambiguous position: on the one hand it plays the role of a controller towards the job seekers, on the other hand it assumes to be processor acting on behalf of the controllers, such as Enterprize Inc and other companies seeking staff through it.

- Furthermore, Headhunterz - with its famous value-added service "global matchz" - looks for suitable candidates both among the CVs received directly by Enterprize and those it already has in its extensive database. This ensures that Headhunterz, which according to the contract is paid only for contracts actually signed, enhances the matching between job offers and job seekers, thus increasing its revenues.

- In spite of the contractual qualification, Headhunterz Ltd shall be considered as a **controller**, and as **joint controller** with Enterprize Inc at least those sets of operations relating to Enterprize recruitment.
  - WP 169 at 19

BRYAN CAVE LEIGHTON PAISNER BCLP

Data Pool

- PlumbUP has created a new phone application to organize gatherings of plumbers throughout the EU. PlumbUP is working with two other entities, the French Plumbers ("FP") and German Plumbers ("GP"). FP and GP will contract with PlumUP to access the PlumbUP platform in order to provide plumbers country specific materials. PlumbUP hopes to sign up entities similar to FP and GP around the world.
- This is a **Joint Controller** relationship
  - Each party is making decisions around the purpose and means of processing, so no party can be a processor
  - FP and GP are not separately determining the purpose and means of processing in a way that would make them separate controllers
    - PlumbUP decides what information is gathered through their platform, possibly with input from FP and GP
    - The means of processing remain almost exclusively with PlumbUP

BRYAN CAVE LEIGHTON PAISNER BCLP

Travel Agency

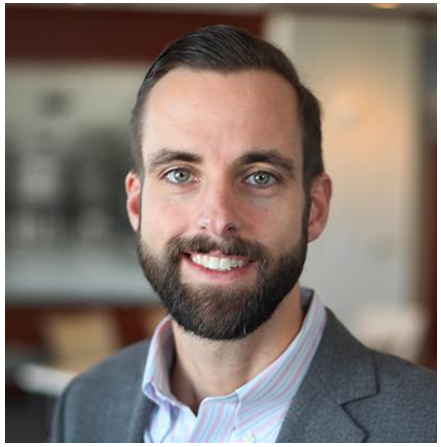
- A travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers.
  - Here, the travel agency, the airline and the hotel will be three separate data controllers, each subject to the data protection obligations relating to its own processing of personal data. (WP 169 at 19)

Travel Agency 2

- The travel agency, the hotel chain and the airline decide to set up an internet-based common platform in order to improve their cooperation with regard to travel reservation management. They agree on important elements of the means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out integrated marketing actions.
  - Here, the travel agency, the airline, and the hotel chain, are joint controllers with regard to the processing operations relating to the common internet-based booking platform. However, each of them would still retain sole control with regard to other processing activities, e.g. those relating to the management of their human resources. (WP 169 at 19)

BRYAN CAVE LEIGHTON PAISNER BCLP

Biographies



Sean Christy

Sean.Christy@BCLPlaw.com

- Sean is a trusted business and legal advisor to many public and privately-held companies in complex sourcing, cloud and other technology arrangements and related automation (artificial intelligence and robotic process automation) arrangements.
- Sean represents clients in their most critical initiatives, ranging from global transactions by multinational corporations to the core business deals of early stage start-up companies.
- www.linkedin.com/in/sean-christy-8535564

Tyler Thompson

Tyler.Thompson@BCLPlaw.com

- Tyler is an attorney and International Association of Privacy Professionals "Fellow of Information Privacy" (FIP), as well as a Certified Information Privacy Professional for the United States and Europe (CIPP/US, CIPP/E) and Certified Information Privacy Manager (CIPM), in the Technology, Entrepreneurial, and Commercial practice of Bryan Cave Leighton Paisner.
- Tyler's practice focuses on technology transactions and data privacy and security matters. Previously, Tyler worked for two Fortune 500s, a startup, and the University of Colorado.
- www.linkedin.com/in/tylerjthompson
- www.bclplaw.com/en-US/practices/corporate/data-privacy-and-security-team/index.html

BRYAN CAVE LEIGHTON PAISNER BCLP

BRYAN
CAVE
LEIGHTON
PAISNER

BCLP

bclplaw.com