

CONTROLLER OR PROCESSOR?

Guidelines on Data Processing Roles for HR Service Providers



Content

Disclaimer	Page 2
Introduction	Page 3
Data processing roles in relation to HR Services	Page 3
Controller or Processor	Page 4
○ Data Controller	Page 4
○ Data Processor	Page 5
○ Purpose and Means of Processing	Page 5
The Three Data Processing Relationship Types	Page 6
○ Controller-Controller	Page 6
○ Controller-Processor	Page 6
○ Joint Controller	Page 7
○ Further Reading	Page 8
Applying the Data Privacy Roles to HR Services	Page 9
○ Temporary Agency Work	Page 10
○ Payrolling and Employment of Record	Page 15
○ Direct Recruitment	Page 17
○ Recruitment Process Outsourcing (RPO)	Page 19
○ Outplacement/Career Management	Page 20
○ Managed Service Provider (MSP)	Page 22
○ Master Vendor (MV)	Page 25
About the World Employment Confederation	Page 27

IMPORTANT

Before you begin your review of this document, please note that pages 2-8 provide background information and guidance on the relevant general concepts of the GDPR regulation. These sections are useful if you are looking to educate yourself on the topic of data processing roles under GDPR.

If you are simply looking for specific guidance in relation to a certain HR Service, this information can be found on pages 9-17. See the table of contents on pages 1 or 9 to find the section you are looking for.

DISCLAIMER

Nothing in this document should be construed as legal or professional advice, nor as a replacement for obtaining the appropriate legal or professional advice.

The purpose of this document is to provide general and non-specific guidance on the data privacy relationships of the direct parties across a selection of HR Services. The HR Services described in this document may or may not align with the specific services provided by our members. Also note that the actual conditions and circumstances of the service provided dictates how GDPR is applied.

Note that GDPR is still a fairly new regulation, and its application is subject to the individual practice and interpretation of the in-country data protection authorities (DPA) and courts across Europe. Accordingly, we cannot guarantee that the content of this document completely aligns with any future application and/or interpretation of the GDPR by the DPA and/or courts in your country.

The contents in this document do not create any regulatory framework and complying with it is not mandatory nor binding with respect to HR Service providers and/or their clients. In addition, we've added a few references following the publication of the guide to recruitment by the CNIL¹ (French supervisory authority), officially published in 2023. The World Employment Confederation (WEC) shall not be relied upon to enforce the guidance provided in this document with respect to its members.

All WEC members are liable for their own decisions, actions, and omissions. While the WEC endeavours to ensure that the information contained in this document is accurate at the time of publication, the WEC does not accept any responsibility or liability for the accuracy, content, completeness, legality, or reliability of the information contained in this document, nor does the WEC accept any responsibility or liability for any action or inaction taken by our members or third parties on the basis of the guidance contained herein.

¹ The guide is freely available for consultation (in French) on the CNIL website:
https://www.cnil.fr/sites/cnil/files/atoms/files/guide_referentiel_-_recrutement.pdf

Introduction

The private employment industry acts as a labour market intermediary by matching labour market supply with labour market demand. It does this by providing a broad spectrum of services such as temporary agency work, payrolling, employment, direct recruitment, managed service provider (MSP), HR outsourcing and consulting services, and other similar services (collectively “**HR Services**”).

Given the nature of HR Services, it almost always involves the processing of personal data and the exchange of that data between two or more parties. HR Service providers and their clients should be aligned when it comes to the assessment of their data protection roles as either a *Controller* or *Processor* of that personal data in accordance with the General Data Protection Regulation of the European Union (“**GDPR**”).

We hope that this document is able to help you identify your data protection/GDPR roles with respect to the provision and/or receipt of the HR Services.

GDPR Data processing roles in relation to HR Services

When a company is engaged by a client to perform HR Services, the relationship is usually formalised by the parties entering into an agreement for such services. This agreement will generally identify the various HR services in scope of the relationship and can be used as a starting point for assessing how the data processing roles of Controller and/or Processor should be allocated.

Sometimes the HR Services provider and their client will also enter into an additional data processing agreement, specifically regulating and/or describing the processing of personal data in the relationship. This may provide further clarification on the obligations and responsibilities of the parties.

It should be noted that the GDPR takes precedence over any agreement between the parties. This could be the case if the contract includes a misapplication of the law, or if the factual relationships or circumstances between the parties are not represented correctly. For example, any clause stating that one party is a Controller or a Processor would be void if this does not align with the actual relationship between the parties.

Once the relationship is clarified and established, it is important to note that the assigned roles come with a set of obligations, which are outlined in the GDPR legislation. These obligations will not be covered in detail by these guidelines. For more information about your obligations as a Controller or Processor, we advise you to consult the website of the European Data Protection Board and/or your national Data Protection Authority (DPA). An overview of national DPAs can be found by following this link:

Your national association might also be able to provide further support on GDPR implementation and compliance in the HR Services industry in your country.

Controller or Processor

Data Controller

A Controller is the party that *makes decisions and exercises control* with respect to the essential elements of the data processing, including the *purposes and means* of processing. The role of Controller may be established by law or may be determined by analyzing the factual elements or circumstances of the data processing in question.

An organization may be considered a Controller under GDPR, even if their operations does not deliberately target personal data. It should also be noted that any company who wrongfully determines that they are *not* a Controller, will still be held accountable for their obligations as a Controller under GDPR. For this reason, it's very important that any conclusions about whether or not a party is a Controller are accurate.



There is no limitation as to the type of entity that may assume the role of a Controller, but it is usually an organization that acts as a Controller, and not an individual within an organization. Existing traditional roles and professional expertise that normally imply a certain responsibility will often help in identifying the Controller. For example, an employer in relation to their employees, a publisher processing personal data about its subscribers, or an association to its members or contributors will in most cases be the Controller for such processing.

In many cases, the terms of a contract can help identify the Controller. However, contracts can be inaccurate or even wrong. In fact, they can actively mislead the analysis in some cases. If you are struggling to identify the Controller, you can ask two basic questions:

1. Who decided that this processing should occur?
2. Who decided how that processing should occur?

In most cases the answer to question 1 and 2 should be the same and should give you the identity of the Controller. If the answers to questions 1 and 2 are different, deeper analysis is likely needed. You may be looking at a Joint Controller situation. More on that further below.

IMPORTANT: One person may have their personal data processed by several parties, for several purposes, and using several different means of processing. Accordingly, there could be several Controllers and Processors operating in a chain or matrix of data processing activities related to the same personal data.

Data Processor

A Processor is a person or entity which processes personal data on behalf of the Controller. Two basic conditions for qualifying as a Processor exist:

1. That it is a separate person and/or legal entity from the Controller.
2. That it processes personal data on the Controller's behalf.

The Processor must only process the data in accordance with the Controller's instructions. However, when a Controller engages a Processor to carry out the processing on its behalf, the Processor is often still able to make certain decisions about how to carry out the processing, for example how to implement and comply with the Controller's instructions from a technical perspective (e.g. which staff to utilize, which hardware/software to use).

In order to engage a Processor under a Controller, a written and legally binding data processing agreement must be established between the parties, setting out the Controller's instructions and the Processor's obligations under GDPR.

IMPORTANT: Note that two departments of the same legal entity cannot act as Controller or Processor to each other, nor can an employee act as a Processor of their employer. However, separate legal entities within one larger group of companies can still act as Controller or Processor in relation to each other.

Purposes and means of data processing

You will often find reference to "*purpose*" and "*means*" in relation to personal data processing. The GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the purposes of the processing and the means to achieve them is therefore particularly important when determining the data processing roles of the parties. Dictionaries define "*purpose*" as *an anticipated outcome that is intended or that guides your planned actions*. They define "*means*" as *how a result is obtained or an end is achieved*. Accordingly, purposes and means of processing can be described as the "*why*" and the "*how*" of personal data processing.

Purpose = *Why* is the data being processed?

Means = *How* is the data being processed?

The Three Data Processing Relationship Types

Three primary data processing relationships exist under the GDPR:

1. Independent Controllers
2. Controller to Processor
3. Joint Controllers

Controller to Controller relationship (Independent Controllers)

The Controller to Controller relationship exists when two parties exchange personal data for which they independently act in the capacity of Controller. The parties are *Independent Controllers*. This means that they do not process the personal data on behalf of each other. Two Independent Controllers may process the personal data of the same data subjects, but they both do so for their own purposes. Each party generally uses its own database and IT tools. One party may send personal data to the other from time to time (absence of synchronization), to achieve its own purpose or to enable the other.

Although a data processing agreement is not legally required in this relationship, agreeing on some data processing terms might be helpful to clearly identify and affirm the Controller to Controller relationship. This can be set out in a short and simple set of contractual clauses within any relevant agreement between the two Controllers, as it does not need to be as detailed as a full data processing agreement. Failures of one party to comply with the GDPR do not impact the compliance of the other.

EXAMPLE: Temp Agency Work and Direct Recruitment (see further below) can be examples of a HR Services provider acting in a Controller to Controller relationship with their client.

Controller to Processor

In this relationship, the Controller engages the Processor to process personal data on their behalf. The Processor is a separate legal entity from the Controller, and it processes personal data in accordance with specific purposes and means, which are determined by the Controller. The Processor processes data exclusively to meet the needs of the Controller (*e.g.* to recruit a candidate) and does not have a specific purpose of its own.

Under the GDPR, this relationship must be formalized in an agreement or law that is binding on the Processor and enforceable by the Controller. This agreement should particularly set out the following *for each processing activity*:

- **Subject matter** and **duration** of the processing
- The **nature** and **purpose** of the processing
- The **type of personal data** and **categories of data subjects**
- The **obligations** and **rights** of the Controller

EXAMPLE: MSP & RPO can be examples of a HR Services provider acting as a Processor for a client.

Joint Controllers

When two or more Controllers *jointly* determine the purpose and means of the processing of personal data, they are deemed Joint Controllers. Joint Controller relationships are not common within the area of HR Services, although they do exist.

IMPORTANT: Please note that while the Controller is primarily responsible for compliance with GDPR in this relationship, both parties can either *jointly or independently* be found liable for breaches of GPDR. For example, *both* the Controller and Processor are independently responsible for ensuring that appropriate technical and organizational measures are put in place to protect the personal data they are processing.

Not all data processing involving several entities give rise to Joint Controllershship. The overarching criterion for being Joint Controllers is the participation of two or more entities in the determination of the purposes and means of processing. If both the purposes and means are collaboratively determined by more than one legal entity, they should be considered joint Controllers for the processing in question. The existence of joint responsibility does not necessarily imply equivalent responsibilities between Joint Controllers. Recruitment players may be involved at different stages of the processing operation, and to different degrees². Joint Controllers should set up an arrangement that sets out their respective responsibilities in relation to each other. The essence of the arrangement must be made available to the data subject. The entities must both determine the purpose(s) and essential means of the processing, or at a minimum, be able to intervene in this determination. If an entity is not able to determine the purpose or the essential means (processed personal data, retention periods, recipients, etc.), it cannot be considered a joint data controller.

Note that Joint Controllers are each independently liable for their breaches of GDPR, regardless of what arrangements they have made between themselves. Irrespective of the terms of the arrangement, data subjects may exercise their rights with respect to each of the Joint Controllers. Supervisory authorities are also not bound by the terms of the agreement between the Joint Controllers and can exercise their authority over both parties regardless of any division of responsibilities they have set out between themselves.

EXAMPLE: A Service provider and their client managing a shared talent pool in a shared system could be an example of Joint Controllershship.

IMPORTANT: It might seem difficult to distinguish between being Joint Controllers and having a Controller-to- Controller relationship. The key difference is that Joint Controllers generally *jointly* determine shared purposes and means of processing, while Independent Controllers will always determine their own *separate* purposes and means.

² CNIL Recruitment Guide - Sheet No. 3, p. 19

Further reading on 'Controller' and 'Processor':

- UK Information Commissioner's Office guidance on Controller and Processor: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/>
- European Data Protection Board guidance on Controller and Processor: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf










Applying the Data Privacy Roles to HR Services

These guidelines cover the most common HR Services. Note that there exists additional HR Services that are not directly covered by this list. A factual analysis in line with the principles explained in this document should be applied to those services to determine the relevant data processing roles and responsibilities.

Also note that exceptions to the below guidance is possible. Always conduct a thorough factual analysis of your client relationships before determining what data processing roles the parties have in relation to each other.

IMPORTANT: In some cases, a client and an HR Service provider can make special arrangements with respect to the below listed services, e.g. a client may instruct the HR Service provider to do data processing activities on their behalf (for example by managing candidates in a separate client-owned system, solely for the client’s purposes). So even if the HR Service provider is a Controller, they may act as a Processor for such certain arrangements with a client.

These guidelines explicitly cover the most common arrangements within the following HR Service product groups:

						
Temporary Agency Work	Payrolling & Employment of Record	Direct Recruitment	Recruitment Process Outsourcing (RPO)	Outplacement / Career Management	Managed Service Provider (MSP)	Master Vendor (MV)
Page 10	Page 12	Page 13	Page 14	Page 15	Page 16	Page 18

Temporary Agency Work (Staffing)

Temporary Agency Work (often referred to as “staffing”, “worker leasing” or “agency work”) occurs when a company delegate (borrows) one or more workers from a HR Service provider, often referred to as a staffing agency, on a temporary basis. Staffing has a triangular structure, where the staffing agency signs an employment or engagement contract with a worker and then places the worker with their client to perform work for that client. The agency worker generally performs their work duties in a manner similar to that of an employee of the client.



A common misconception when it comes to data privacy roles in staffing relationships is that one of the parties acts as a Processor of the other. This is generally not the case.

Please note that CNIL has clarified the roles at stake with respect to the recruitment process through the fiche 3³. The qualification of data processor, data controller, or joint controller is determined on a case per case basis. If a player decides the purposes and the means of the data processing, he is the data controller.

Usually, when a client retains a staffing agency to provide them with temporary workers, the staffing agency is the party that sources the workers and obtains their personal data. Sometimes they even have suitable candidates in a pre-existing talent pool or database. The staffing agency may freely match these candidates with multiple clients. The staffing agency also decides how to process and store the information. Accordingly, they have determined the purpose and means of the processing, completely independently from their clients. Once a candidate has been selected for engagement by a client, the agency usually becomes the candidate’s employer, which further indicates that the agency is a Controller.

Once suitable candidates have been identified for roles with a client, the candidates’ personal data is shared with the client by the staffing agency. The client then processes the candidates’ personal data in order to select and engage temporary worker(s) to perform work duties for them. The client is necessarily recipients of some of the personal data of temporary employees made available by agency, (i.e., data that is strictly necessary for ongoing workforce management purposes) and become Controller for data processing that they themselves create from personal data received from agency. Client is also Controller for processing the data they subsequently collect in view of the work organization systems they deploy within their organization which involve the processing of personal data (e.g.: time clock, video surveillance)⁴. This indicates that the client is *also* acting as a Controller with respect to both, the candidates and the workers. Any personal data not necessary for the achievement of the intended purpose and in compliance with the applicable labor law (namely the delegation of the temporary employee by the agency to the client) cannot be communicated to the client, unless a legal provision (particular applying specifically) is respected. Concerning the application of specific French law, the CNIL has drawn up a list of information that can be communicated to the customer.

The staffing agency and their client are processing the same data subjects for purposes that are closely linked, but *not the same*. They also determine their own means of processing (e.g. which HR systems to use). In summary, both client and agency have their own independent legal bases and purposes for the processing of the workers personal data.

³ CNIL Recruitment Guide - Sheet No. 3, p. 11

⁴ CNIL Recruitment Guide - Sheet No. 3, p. 16

CONCLUSION: The parties are *Independent Controllers*; the staffing agency is the Controller for their own processing and the client is the Controller for their own processing. This means that *both* parties – separately – have to ensure that they are processing the data in a manner consistent with GDPR requirements.

IMPORTANT: Staffing agency workers are often required to process personal data as part of their work duties with a client. As this processing happens under the supervision, direction and control of the client, using the client’s own systems and processes, it’s clear that the worker is acting in a manner that is consistent with the client’s own employees. The staffing agency is generally not involved in this data processing at all. Accordingly, the worker performs these tasks as a part of the client’s organization, and no Controller-Processor relationship is established as a result of workers performing data processing activities while assigned to a client.

IMPORTANT: Note that this guidance will essentially also be applicable for staffing agencies that place *independent contractors*, although the role of the independent contractor themselves must be determined based on a factual analysis of the scope and nature of the services they provide.

IMPORTANT: Bear in mind that you will have to assess the roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service provider can still be considered a Processor for their client with respect to certain processing activities, even if they are acting as a Controller in other respects.

FOR EXAMPLE:

HR Service provider processing activity A: Sourcing and employing temporary workers

Role: **Controller**

HR Service provider processing activity B: Managing a client-owned talent pool in client’s HR system

Role: **Processor**

Payrolling and Employer of Record

Payroll suppliers (e.g. a payrolling agency or an umbrella company) may be engaged by a client to manage and process their workers' payroll and/or employment responsibilities. This may for example be practical if a company needs to hire personnel in a country where they lack a legal entity. They can then engage in-country staff using a local HR Service provider.



The services provided by the payroll supplier determine to what extent it acts as a Processor or a Controller. For example, if it receives personal data from their client and is merely asked to calculate and remit pay, then it is a Processor of their client. On the other hand, if the payroll supplier is the employer of record for the agency worker, then it acts as a Controller in its capacity as the employer. Bear in mind that its possible for a payroll supplier to be a Controller in their capacity as employer of record, but to still act as a Processor of their client for the other aspects of their service.

CONCLUSION: With the above in mind, it's reasonable to make the assumption that a payroll provider or employer of record acts as a Processor of their client, at least to a certain extent. For instance, an employer of record will generally always process the personal data of workers, and provide associated reports, documentation and notifications to the client, subject to the directions and requirements of such client. This would make them a Processor, while the Client is the Controller. However, when the HR Service provider process the engaged staff's personal data for the purposes of acting as an employer (e.g. calculating and remitting income tax or procuring legally required employee insurance), they are acting in their capacity of employer and they are the Controller.

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Controller for certain processing activities, even if they are primarily a Processor for their client.

FOR EXAMPLE:

HR Service provider processing activity A: Acting as an employer for temporary workers

Role: **Controller**

HR Service provider processing activity B: Payrolling their client's workforce

Role: **Processor**

Direct Recruitment



Direct recruitment involves the HR Service provider identifying and shortlisting of candidates for the purpose of matching them with an open role with one or more of their clients.

When a client engages a recruitment agency to provide them with candidates for an open role, the agency is the party that sources the candidates and obtains their personal data. They will often have suitable candidates in a pre-existing talent pool or database. The agency may freely match these candidate profiles with multiple clients. The recruitment agency also decides how to process and store the personal information irrespective of their clients. Accordingly, they have determined the purpose and means of processing. This means that the recruitment agency generally is a Controller, even if they are retained by a client to do a specific candidate search. Thus, if the agency goes looking for a specific candidate for the client, that it will only process the data necessary for the client as part of its own recruitment and that it will not process the candidate's data subsequently for its own databases (agency's pool of talent), it could be considered as a processor.

Once suitable candidates have been identified, their personal data is shared with the client by the recruitment agency. For the recruitment agency, the candidates are their product and they are processing their personal data in order to operate their business and to maintain a pool of talent. The client, on the other hand, is processing the candidates' personal data in order to select and hire one or more of them as direct employees. The two parties' purposes for processing the personal data are linked, but not the same. This means that the client and the HR Service provider are both Controllers for their own processing of the personal data.

CONCLUSION: The parties are *Independent Controllers*; the recruitment agency is the Controller for their own processing and the client is the Controller for their own processing. This means that *both* parties – separately – have to ensure that they are processing the data in a manner consistent with GDPR requirements.

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Processor for their client with respect to certain processing activities, even if they are primarily a Controller.

FOR EXAMPLE:

HR Service provider processing activity A: Sourcing candidates for current and future clients

Data Privacy Role: **Controller**

HR Service provider processing activity B: Managing a client -owned candidate pool in client's HR system

Data Privacy Role: **Processor**

Recruitment Process Outsourcing (RPO)



Recruitment Process Outsourcing (RPO) occurs when a client *outsources* all or part of its internal talent acquisition or recruiting function to a HR Service provider who offers RPO services.

While similar to direct recruitment, RPO means that the HR Service provider is performing its search and selection activities *in the name of their client*. For the average jobseeker, communicating with an RPO provider about a role will be no different from communicating directly with the prospective employer directly. They will generally see the client's logos, email addresses and privacy notices, and not those of the RPO provider. The client will have full ownership of all candidates sourced through their RPO and the RPO provider generally cannot match candidates with additional clients. The RPO activities should ideally be separated from the other activities of the HR Service provider, utilizing separate employees and systems (or using client systems). The RPO provider, in essence, acts as a recruiting arm of their client.

CONCLUSION: In an RPO as described above, it is generally always the client who determines the means and purposes of the personal data processing. This makes the client the Controller and the RPO provider their Processor.

Note that while the above is accurate for *true* RPO, there are many instances of HR Service providers who provide products that are referred to as RPO services, but that align more closely to staffing or direct recruitment (e.g. project resourcing). If the recruitment activity is done in the HR Service provider's own name, it's not actually RPO as defined in this document. In this case, the specifics of the service should be analysed to see whether it aligns better with direct recruitment.

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Controller for certain processing activities, even if they are primarily a Processor for their client.

FOR EXAMPLE:

HR Service provider processing activity A: Managing an internal candidate pool for use across several RPO programs

Data Privacy Role: **Controller**

HR Service provider processing activity B: Recruiting staff as the client's talent acquisition team

Data Privacy Role: **Processor**

Career Management / Outplacement

Career management and outplacement services typically support clients who are reducing their internal workforce. The HR Service provider supplies labour market tools, training, financial planning, social security navigation, career advice and other forms of support to workers who are looking for new employment as a result of the workforce reduction. The purpose of the service is to help the displaced workers make a successful transition to the labour market and find new ways to support themselves. These services usually commence once the worker has been informed that their roles will be terminated and continues for a set period into their unemployment.



Typically, the workers involved are employed by the client as the outplacement services are performed. It's clear that the client acts as a Controller in this regard, determining their own purposes and means of processing for their employees (and former employees).

CONCLUSION: The service of career management and unemployment advice is directed at the individual workers. Most commonly, the HR Service provider determines their own purposes and means of processing the personal data of these workers while performing the service, making them a Controller. Exceptions to this rule can't be excluded, depending on the specific nature and scope of the service and the agreements between the HR Service provider and the client. As always, a factual analysis of the relationship is recommended before determining the respective data privacy roles of the parties.

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Processor for their client with respect to certain processing activities, even if they are primarily a Controller. For example, if the client asks the HR Service provider to perform exit interviews on behalf of client HR and log them in a client system, the HR Service provider would be acting as a Processor of the client with respect to that activity.

FOR EXAMPLE:

HR Service provider processing activity A: Providing ongoing career advice for the benefit of displaced workers

Data Privacy Role: **Controller**

HR Service provider processing activity B: Performing exit interviews for the benefit of the client's HR

Data Privacy Role: **Processor**

Managed Service Provider (MSP)

MSP involves the outsourcing of HR and procurement activities from a client to an HR Service provider (the MSP) in an “MSP program” – a predefined set of rules, systems and procedures. MSP programs generally manage or administrate certain categories of service providers and the associated service delivery on behalf of their clients. The MSP program is usually managed by means of an electronic procurement management system and often spans several sites, locations, and even countries.



Crucially, the MSP does not deliver the managed services to the client itself. The services are rendered by means of the managed or administrated service providers. The MSP acts as either an intermediary or third-party administrator.

MSP programs can include the management of almost any kind of service provider, including other HR Service providers or statement of work service providers. For the purpose of this document we will focus on MSP programs that manage other HR Service providers, but the same principles should in most cases be applicable for other categories of MSP programs as well.

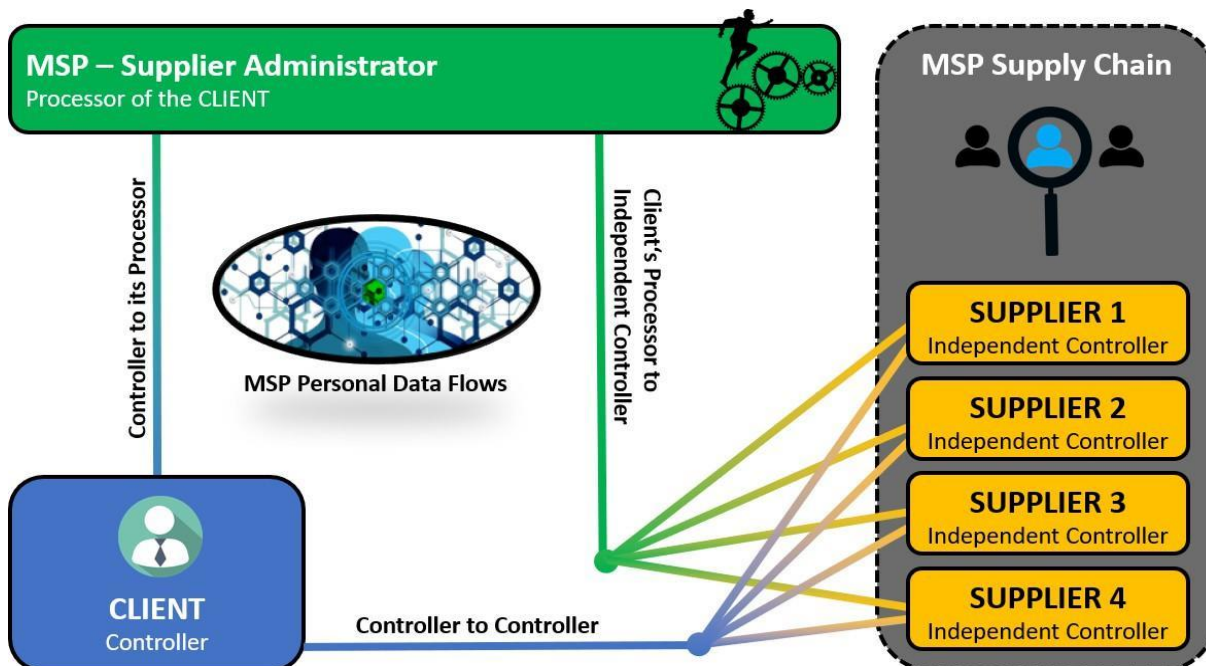
Managed service provider programs can be set up in a variety of different structures and contracting models. It is important to note that the actual facts of the relationship determine the roles of the parties in connection with each individual processing activity. The most common structures will be covered here, but thorough business process analysis by a GDPR expert is recommended when designing and implementing an MSP.

It should be noted that the lack of a service contract between the client or MSP and the suppliers does not necessarily preclude that a relationship exists from a data privacy perspective. This should be taken into account when analysing the relationships and roles in an MSP. If two of the parties exchange personal data, a data privacy relationship exists even if there is no formal contract to establish it.

Since an MSP program is an *outsourcing arrangement*, the MSP generally acts as an agent or representative of their client, who is the end recipient of the HR Services provided by the MSP supply chain. From this it follows that the client generally determines the purposes and means of the personal data processing and is a Controller, while the MSP is a Processor for the client.

From a data privacy perspective, the suppliers in the MSP program operate the same way as regular staffing agencies in that they also generally determine their own purposes and means of data processing with respect to candidates and workers.

MSP Personal Data Relationships:



CONCLUSION: On the basis of our above analysis, it's clear that both the client and the individual service providers in the supply chain are Controllers for their own processing. It also follows that the MSP is the Processor of the client in most cases. *However, this is where a thorough factual analysis is needed.*

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Controller for certain processing activities, even if they are primarily a Processor for their client.

FOR EXAMPLE:

HR Service provider processing activity A: Creating data analytics to assess internal performance across clients

Data Privacy Role: **Controller**

HR Service provider processing activity B: Managing suppliers and worker assignments for the client

Data Privacy Role: **Processor**

In general, the MSP acts in the interest of their client, and it's usually clear that the MSP is that client's Processor. However, in exceptional cases, if the MSP holds the contracts with the service providers in the supply chain and acts on their own authority with a large degree of autonomy with respect to the engagement of suppliers and individual workers, it can be argued that the MSP can also be a Controller. Note that if the MSP collects and processes personal data for their own purposes (e.g. for internal data analytics), they will be a Controller for that specific processing activity, regardless of their broader role in the MSP Program.

Master Vendor (MV)

Master vendor (MV) involves a client engaging a HR Service provider to be the primary supplier of one or more categories of temporary workers, with several additional secondary suppliers acting as subcontractors to the MV. Usually, no direct contractual relationship exists between the client and the secondary suppliers.



The MV will generally attempt to fill most of the client’s open roles themselves, acting similarly to a regular staffing agency. However, they will often rely on their secondary suppliers to source and provide additional workers. These workers are supplied to the MV, who in turn supply them to the client. The secondary supplier will remain the employer of the individual workers. Similarly to an MSP, some MV programs also use vendor manager technology and include additional data analytics and management functions, blurring the line between MV and MSP.

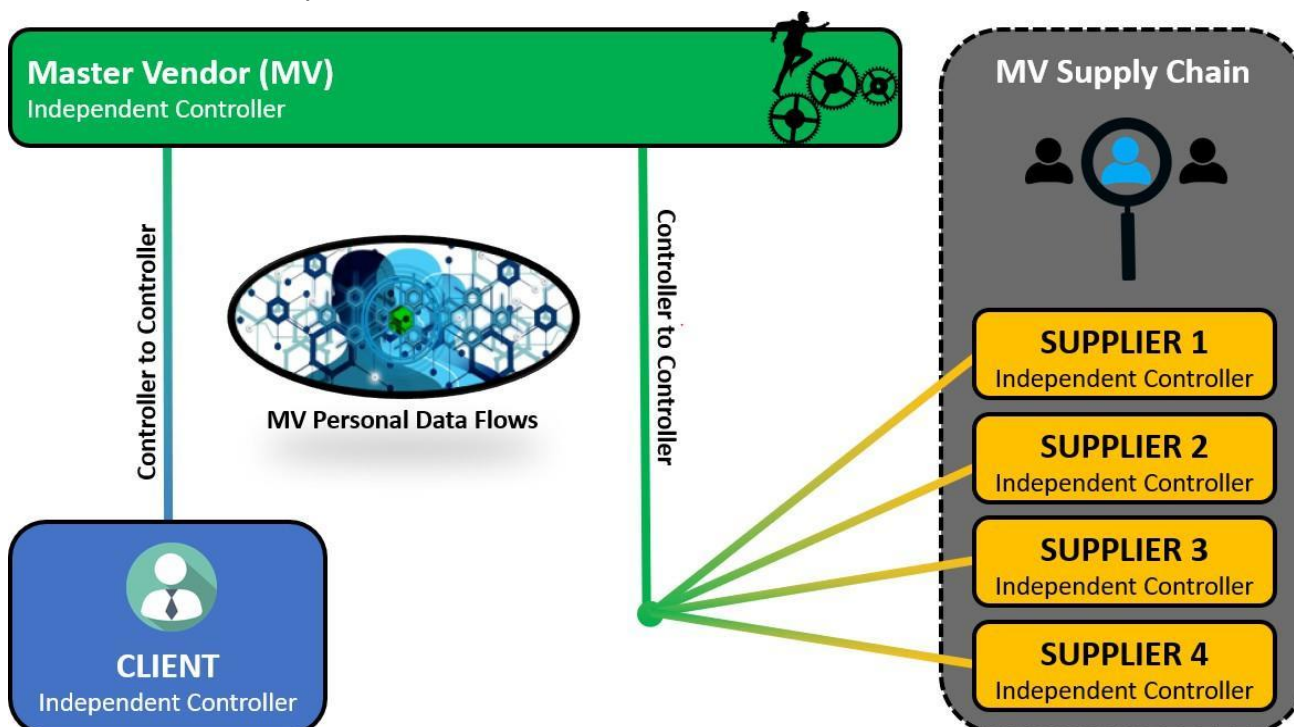
It should be noted that the lack of a service contract between the client and the suppliers does not always preclude that a relationship exists from a data privacy perspective. If the client and suppliers directly exchange personal data, a data privacy relationship exists even if there is no formal contract to establish it. This should be taken into account when analysing the roles and relationships in a master vendor arrangement.

In an MV arrangement, the client clearly determines their own purposes and means of processing and acts as a Controller while assessing, engaging and managing temporary workers.

Normally, the master vendor has a significant amount of autonomy with respect to choosing secondary suppliers and which workers they will present to a client. It follows that, in most circumstances, the MV should also be considered a Controller for their own data processing.

From a data privacy perspective, the suppliers in the MV program operate the same way as regular staffing agencies in that they also generally determine their own purposes and means of data processing when sourcing and employing temporary workers.

MV Personal Data Relationships:



CONCLUSION: In most MV arrangements, all three parties are generally Independent Controllers for their own processing in relation to each other.

Note that there may be exceptions to the assumption that all parties in a MV are Controllers. This is dependent on several factors; for instance, if there is a significant degree of control and instruction exercised over the MV by the client, this could indicate that the MV is a Processor in relation to the client. If there are auxiliary services being provided by the MV for the sole benefit of the client, like for instance data analytics or spend reporting, this can also indicate that the MV is a Processor for the client with respect to these activities.

IMPORTANT: Bear in mind that you will have to assess the data privacy roles with respect to each individual processing activity (or each group of similar processing activities). This means that the HR Service Provider can still be considered a Processor for their client with respect to certain processing activities, even if they are primarily a Controller.

FOR EXAMPLE:

HR Service provider processing activity A: Collecting data analytics to assess internal performance across clients

Data Privacy Role: **Controller**

HR Service provider processing activity B: Doing supply chain audits for the client

Data Privacy Role: **Processor**

About the World Employment Confederation

The World Employment Confederation serves as the voice of the HR services industry at the global level, representing both national federations and workforce solutions companies worldwide. Our diverse membership encompasses a broad spectrum of HR services, including agency work, direct recruitment, career management, Recruitment Process Outsourcing (RPO), and Managed Service Provider (MSP) solutions.

Our mission revolves around securing recognition for the pivotal role played by the HR services industry in fostering well-functioning labour markets and advocating on behalf of our members to enable appropriate regulation. By fostering an environment conducive to sustainable growth of the HR services sector, our ultimate goal is to deliver better labour market outcomes for all.

By bridging the supply and demand gaps in labour markets, creating pathways to employment, enabling agile organisations, balancing flexibility with protection and deploying digital solutions responsibly, the HR services industry plays a central role in addressing labour market challenges and delivering people-centric solutions.

Find out more :

www.wecglobal.org