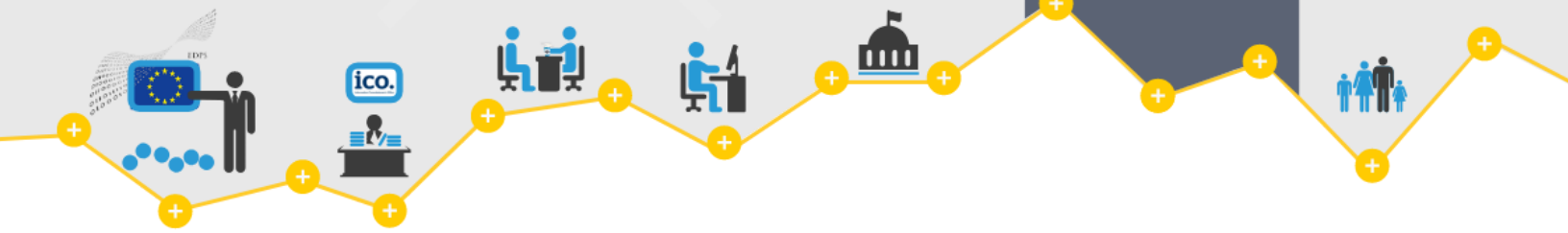
THE GDPR

LEGITIMATE INTEREST ASSESSMENT



"Do I have a ***Legitimate Interest*** for processing personal data under GDPR?"

This is one of the most common questions among recruiters getting their databases in order for GDPR.

This pack will help you to answer that question. Inside, you will find:

- when to process personal data on the basis of Legitimate Interest;
- the limitations of using a legitimate interest claim;
- a complete **LIA** self-assessment form, which you can use to demonstrate compliance to clients, partners, and authorities.

eBoss+
RECRUITMENT SOFTWARE

GDPR for recruiters: Legitimate Interest Self-Assessment Pack

One of the most persistent challenges of the **General Data Protection Regulation** is choosing how to assess your obligations when it comes to an existing database.

One thing is almost guaranteed: with no *Grandfather Clause* in **GDPR** to exempt existing data, some action will almost always need to be taken if you wish to prove the compliance of your old data.

What is less clear is the nature - and the extent - of the action you must take.

Legitimate Interest: knowing your options

This has led to confusion, with some recruitment agencies believing that they are required to re-paper entire databases and obtain fresh consents, while others cite a *Legitimate Interest* as grounds for continuing to process their old data.

Unfortunately, **there is no definitive answer** to this question. At the time of writing, the terms of what constitutes a legitimate interest have not been specifically defined by either the UK Information Commissioner's Office (ICO), nor the EU Article 29 Working Party (WP29). It means that a legal resolution would be open to interpretation if you relied on legitimate interest and that basis was subsequently brought into question.

Obviously, this is not ideal for businesses like yours, which require a definitive answer before May 25th. Increasingly, enterprises are finding that they must opt for one of two compromise choices:

1. Re-paper your data subjects in an attempt to process based on *consent*; stand to lose a large portion of your existing database due to non-responders; but guarantee GDPR compliance to even the strictest interpretations.
2. Do not re-paper; rely on *legitimate interest* to retain your existing database; prove your legitimate interests; then prepare to demonstrate compliance to cautious clients – or risk losing their custom.

Each option has its own limitations and drawbacks, and it may be unclear which is preferable in any given situation.

For this reason, **eBoss** has produced the following booklet, to offer broad guidelines, as well as an easy-to-use self-assessment form.

When is Legitimate Interest the right route to take?

Legitimate Interest may be implemented where no other basis applies. But implementation requires that you first of all prove the existence of that legitimate interest. You can achieve this by considering a number of diverse factors, including:

- the balance of power in the relationship between the controller and individual data subject(s).
- the origins of your data (ie: whether it was freely supplied by the data subject).
- whether the individual would naturally expect their data to be further processed in this manner.
- whether the freedoms of the data subject may be negatively affected by processing OR not processing.
- whether the standard of goods and services received by the data subject may be negatively affected by processing OR not processing.
- Many other considerations, including whether other bases for processing already exist.

Each consideration will lend weight for, or against, any claim of a legitimate interest. As you can see, each of the above points may help a recruiter who is attempting to bring an existing database into compliance. There may be a compelling case for claiming a legitimate interest for *both* the organisation and the individual, for example. After all, a candidate could miss out on interviews and employment if the data controller fails to process their data. Equally, candidates may have freely shared their personal data, and it can be assumed that they *expect* their data to be used on an ongoing basis: for the purpose of completing a service.

The next step is to prove this, and to then record your findings.

Understanding GDPR, and the Legitimate Interests of Recruiters

A recruiter may find that they are able to process their databases for the primary purpose of their business: finding jobs for their database of contacts. This purpose may represent a demonstrable *balance of interests*, as data subjects could miss out on employment opportunities if their personal data is not processed.

However: just because one outcome represents a legitimate interest for the processing of data, it does not mean that compliance can be assumed. You must assess, and record, your findings.

Equally, not *all* uses and processes for the same data set can be applied, just because one single legitimate interest has been established. It should not be assumed, for example, that an agency which is permitted to process personal data for a jobs search is also permitted to send unsolicited marketing copy without unambiguous and freely-given consent. A **Legitimate Interest Assessment (LIA)** assesses *one* process, carried out for *one* set of data. Additional data sets, additional processes, and additional uses each require a separate, valid basis for processing.

Minimise your processes

This may sound like an imposition on your internal processes. But, in fact, GDPR is an opportunity to re-evaluate the way you are handling your data. One of the foundational principles of the GDPR is to end the unnecessary and arbitrary processing of personal data.

If you get your compliance programme right, it is an opportunity rather than a burden. It may force you to re-evaluate your current operations, and discover efficiencies that you can implement long into the future.

Legitimate Interest and Marketing

[The following section examines the use of Legitimate Interest for the purposes of sending marketing copy. If your organisation does not distribute promotional material, this section may not apply to you. However, some of the processes explained in this part could help to clarify the way that a completed LIA will help your compliance programme.]

Some confusion exists over the use of legitimate interest for marketing purposes. In particular, the following quotation from Recital 47 may have been misapplied by some sources:

"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." **Recital 47, GDPR.**

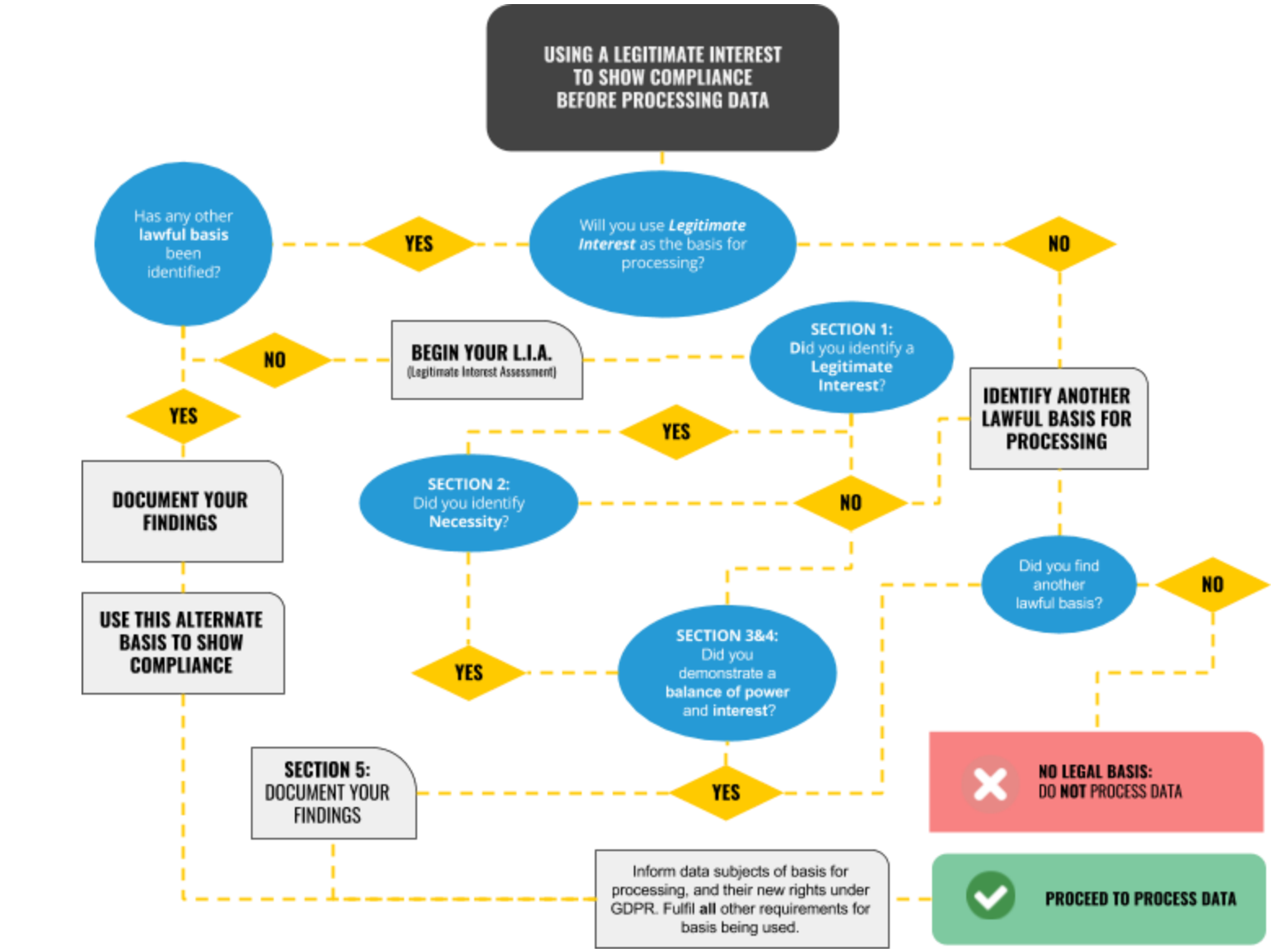
The quote, often used out of content, has left many organisations believing that they can continue to distribute unsolicited marketing copy to individuals on their database. But the legitimate interest here covers only the processing of certain individuals' data, and in specific circumstances; not to the distribution of all marketing material, to any recipient.

For example, an organisation might populate a mailing list due to a *legitimate interest*. However, in order to send advertisements, the organisation should reassess the same data to ensure the *compatibility* of this new use with the original purpose.

Equally, when undertaking any LIA, it will be necessary to record the origins of the data. If the individual did not supply their own data - and is not an existing or previous customer - it could be difficult to establish a balance of interest in terms of a service received, or the expectations of the data subject. In fact in this example, no relationship of any kind would exist between the controller and the data subject. In such circumstances, a legitimate interest would not be easy to establish. Your organisation would struggle to prove a legitimate interest basis for sending promotional material, and would need to seek clear *consents,* to avoid heavy fines.

Your marketing processes must therefore be conducted very carefully. As a recruiter, you must consider how you manage your database in relation to (a) your primary activities as a talent pipeline to clients, and (b) the advertising of your commercial activities to both employers and candidates.

Do not assume that a single, positive LIA self-assessment will provide a basis for processing *all* of your data for *every* purpose. Remember: the minimisation of processing is a cornerstone of the GDPR.


USING A LEGITIMATE INTEREST TO SHOW COMPLIANCE BEFORE PROCESSING DATA
Will you use Legitimate Interest as the basis for processing?
YES
NO
Has any other lawful basis been identified?
YES
NO
BEGIN YOUR L.I.A. (Legitimate Interest Assessment)
SECTION 1: Did you identify a Legitimate Interest?
YES
NO
IDENTIFY ANOTHER LAWFUL BASIS FOR PROCESSING
DOCUMENT YOUR FINDINGS
SECTION 2: Did you identify Necessity?
YES
NO
Did you find another lawful basis?
NO
USE THIS ALTERNATE BASIS TO SHOW COMPLIANCE
SECTION 3&4: Did you demonstrate a balance of power and interest?
YES
SECTION 5: DOCUMENT YOUR FINDINGS
YES
NO LEGAL BASIS: DO NOT PROCESS DATA
Inform data subjects of basis for processing, and their new rights under GDPR. Fulfil all other requirements for basis being used.
PROCEED TO PROCESS DATA

The Legitimate Interest Assessment (L.I.A)

The next section lays out the process of the Legitimate Interest Assessment (LIA). The completed form will help you to demonstrate database compliance to clients and authorities. It requires a special attention to detail, and should be completed for each data set, and for every data process your organisation wishes to carry out.

- Complete the LIA form in its entirety. Record your findings and supply as much specific detail as possible, to inform your conclusions.
- Consider the fact that every LIA is subjective, and that judgements must be made on a case-by-case basis: weigh existing evidence both for and against the processing of data.
- The LIA is just one part of your GDPR compliance obligations. It is fundamental to establishing the basis of a legitimate interest for processing. However, it must be assessed within the wider context of your other obligations under the GDPR, too. An LIA can never override, or cancel out, any other duty or responsibility that you have to your data subjects and clients.
- The data recorded in every LIA should be reviewed and re-assessed on a regular basis.
- Any changes to the method of, or reasons for, the processing of personal data will require the completion of a new LIA.
- Where you find unclear outcomes, or are unsure of your next step, consider seeking expert legal advice before proceeding with any data processing operations.

SECTION 1: Identifying Your Legitimate Interests			
	Task:	**Record Findings:**	**eBoss advises:**
1	Define the purposes of processing this data:		Define and record your reasons for processing this personal data.
2	Identify whether one or more specific business objective relies upon the processing of this data:		If processing is required to complete a lawful business activity and no other basis exists (eg: consent), "legitimate interest" may be viable. Only one legitimate interest is needed for full compliance. However, recording *all* identifiable interests may prove useful later on.
3	Identify one or more specific business objective of any Third Party which relies on the processing of this data:		
4	Explain here if processing is specifically identified as legitimate by GDPR, PECR, or other applicable law:		Specific legislation may provide a legitimate interest, eg: admin tasks relating to employment in GDPR, Article 9(2) (b).

eBoss+ RECRUITMENT SOFTWARE

SECTION 2: Demonstrating Necessity			
	Task:	**Record Findings:**	**eBoss advises:**
1	Explain why the data controller requires this data to be processed:		This may include commercial or legal needs. Ensure that requirements are clearly expressed to the individual data subject. Purposes can be assessed on a case-by-case basis, and considered singularly, or as a whole. Some purposes will offer greater support to a claim of legitimate interest. It is therefore useful to identify all purposes for processing.
2	Explain why other parties require this data to be processed:		
3	Report any other possible ways of achieving this objective:		
4	Explain here if processing is specifically identified as legitimate, by GDPR, PECR, or other applicable law:		

SECTION 3: Balance of Interests: Impact Assessment			
	Task:	**Record Findings:**	**eBoss advises:**
1	List all categories of data being processed:		Remember: special categories of personal data and data relating to a legal minor will require a specific basis for lawful processing.
2	Indicate whether the data subject is likely to expect this processing to occur:	☐ **Yes** ☐ **No** ☐ **Unclear**	In instances when processing may be assumed to occur, impact will likely already be considered and accepted by the data subject.
3	Answer: Could processing risk limiting the data subjects' individual rights or freedoms?	☐ **Yes** ☐ **No** ☐ **Unclear**	
4	Answer: Could processing risk limiting the data subjects' ability to exercise rights or freedoms in future?	☐ **Yes** ☐ **No** ☐ **Unclear**	
5	Answer: Could processing risk causing harm to the individual data subject?	☐ **Yes** ☐ **No** ☐ **Unclear**	
6	Answer: Is processing in the interest of the individual data subject?	☐ **Yes** ☐ **No** ☐ **Unclear**	
7	Answer: Will processing improve the goods or services received by the data subject?	☐ **Yes** ☐ **No** ☐ **Unclear**	
8	Answer: Will the data controller be negatively affected if processing does NOT occur?	☐ **Yes** ☐ **No** ☐ **Unclear**	
9	Answer: Will a third party be negatively affected if processing does NOT occur?	☐ **Yes** ☐ **No** ☐ **Unclear**	

eBoss+ RECRUITMENT SOFTWARE

SECTION 4: Balance of Interests: Impact Assessment

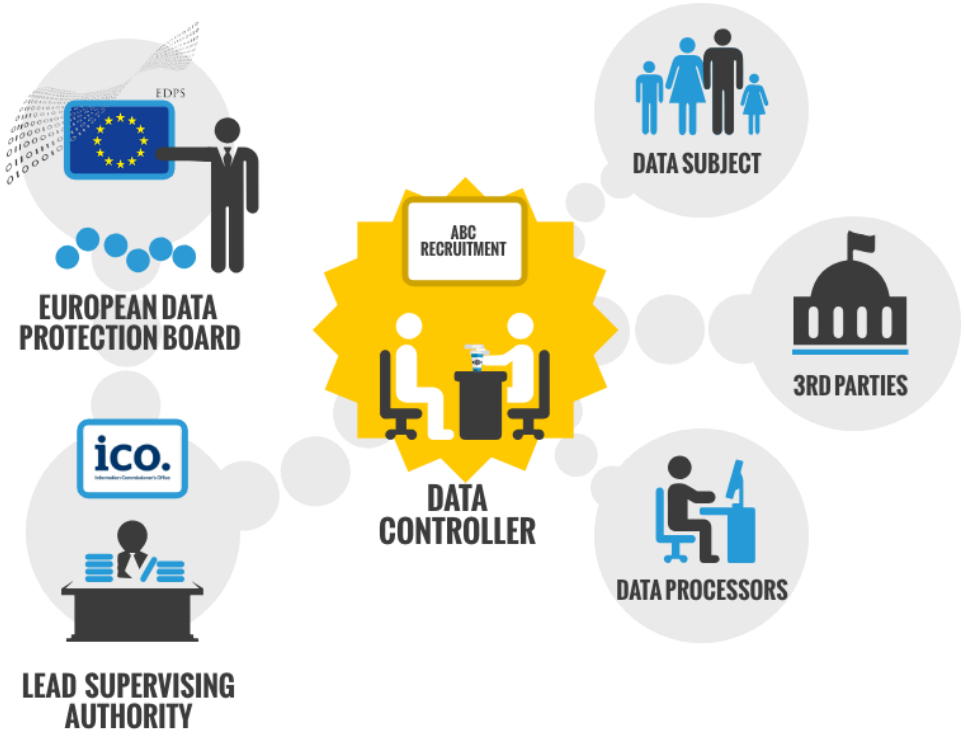
	Task:	Record Findings:	eBoss advises:
1	Describe the basis of the relationship between the data subject and your organisation:		Specify, for example: • Current/former customer / prospect • Employee/contractor • Business client/supplier
2	Describe the nature of the relationship between the data subject and your organisation:	☐ **Direct** (ie: from the data subject) ☐ **Indirect** (source is not data subject) ☐ **Direct & indirect** (mixed data) ☐ **Unclear** (no record)	Specify, for example: if the relationship is permanent, ongoing, one-off, or intermittent.
3	Specify the source of the personal information being processed:		Data collected directly from the subject may lend support for further processing. Indirect data may require more compelling reasons for legitimate interest.
4	Describe the balance of power between the organisation and the individual:		A power imbalance where the individual is in some way obliged to release data for processing is likely to require additional basis for processing.
5	Describe how you make individuals aware that their data is being processed:		If relying on legitimate interest, you should ensure individuals are informed. Notifications should be as complete and specific as possible.
6	Assess whether the individual is likely to expect their data to be processed in this way, within the context of the relationship:		A candidate supplying personal data to a recruiter may likely expect their data to be processed for the purposes of securing interviews / employment.
7	Describe how the individual can control, or object to, the processing of their data:		If the individual has limited or no control over their own data, explain and address this.
8	Identify whether any aspect of the extent of processing may be viewed as unnecessary or inappropriate:		Any processing of unnecessary data could fundamentally undermine the basis of "legitimate interest". Consider ways to minimise your processing. You may refer directly to a previously-completed DPIA for the data subject in this section.
9	Identify ways in which the extent of processing may be reduced to address risks to privacy or freedoms:		

SECTION 5: Self-Assessment Outcomes

eBoss advises: Use this section to assess your LIA findings. Weigh the outcomes of the report, considering the *quantity* of supporting evidence, as well as the *quality and context* of supporting factors. Consider **professional legal guidance** before asserting any basis for, or against legitimate interest.

SIGNED BY	
ROLE	
DATE	

One more hurdle stands in the way of firms using legitimate interest before they can consider their database compliant with GDPR. Now, you must be able to prove your compliance to client businesses and customers who use your services. That includes organisations that may have adopted a strict interpretation of the GDPR regulations surrounding the use of legitimate interest.



If your LIA is called into question, you should be prepared to cite specific examples within your processes and compliance programme, and use specific sections of GDPR regulation to lend substance to your claims (see *"References to Legitimate Interest in the GDPR"*, below). Present your completed LIA for each of your processes, and explain how you have drawn your conclusions: by weighing the balance of interests, and by implementing best practice in relation to privacy and data security.

The rules on Legitimate Interest are not a great departure from their equivalent rules under the Data Protection Act (DPA). As with many other aspects of the GDPR, if you already demonstrate DPA compliance, then you may find the additional GDPR workload is not as great as perhaps first anticipated.

References to Legitimate Interest in the GDPR

The following sections of GDPR make specific reference to grounds of legitimate interest for organisations processing personal data.

- **Article 6(1)(f)**:
  "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
- **Article 13(1)(d)**:
  "Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- **Recital 47:**
  processing for direct marketing purposes or preventing fraud;
- **Recital 48:**
  transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note international transfer requirements will still apply – (see section on transfers of personal data);
- **Recital 49:**
  processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems;
- **Recital 50:** reporting possible criminal acts or threats to public security to a competent authority.

This self assessment pack has been compiled by the **eBoss recruitment** solutions team.

We are a specialist enterprise that develops software products for the recruitment industry. As well as providing an unequalled level of personal support for all of our services, we promote the understanding and adoption of technology-based solutions within the modern jobs market.

Although GDPR represents a significant change in the working culture of many traditional recruiters, it became apparent to us that a lot organisations in the sector were unaware of their new legal obligations, even as the transition period came to an end.

This guide has been written to help organisations such as yours achieve compliance at every step: from laying initial groundwork, to completing the final assessment. It is as relevant for a small start-up as it is for a multinational. You may choose to implement it in part, or in full. Please feel free to share this guide.

David Lyons,
Director, eBoss

When using any of the content of this booklet you are required to acknowledge that GDPR compliance is assessed on a case-by-case basis, and that **no part of this document represents direct or specific legal advice in regard to your organisation's own data protection processes**.

eBoss+
RECRUITMENT SOFTWARE