Legitimate Interests Assessment (LIA)

Version Control	
Document Owner	Simon Pillinger
Document Author	Molly Farrow
Version	1.2

Revision & Approval History			
Version	Date	Author (of revisions)	Summary of Changes
1.0	15/10/2022	Molly Farrow	First version.
1.1	21/10/2022	Simon Pillinger	DPO review.
1.2	26/10/2022	Simon Pillinger	Approved by IGSG. Change to risk 3.

1 Introduction

Legitimate interests is arguably the most flexible lawful basis[1] for processing personal data, it is also one of the most fragile given that the law provides grounds for data subjects to challenge the processing. Legitimate interest assessments (LIAs) assess whether it is appropriate or lawful for an organisation to rely on legitimate interests as a lawful basis for processing personal data. In short they balance the legitimate interests of the data controller and any other parties against the rights and freedoms of data subjects.

LIAs are not a legal requirement and may not be necessary in all circumstances but they are good practice and safeguard individual rights and freedoms as well as the data controller. If the proposed processing requires that a DPIA be conducted then an LIA almost certainly should be conducted because the processing may present a high risk to individuals' rights and freedom. The LIA can form part of the DPIA once completed.

If the processing is contested and brought before either the Information Commissioner's Office (ICO) or a court then not having conducted an LIA is likely to count against the data controller.

2 How to use this Tool

Answer the questions as well as you are able, if you are unsure what a question means, contact Akrivia's Information Governance Manager. Don't panic if you don't know something!

[1] UK GDPR Article 6(1)(f)

3 Project Details

Associated Project
Employee Photography for Marketing Purposes.

4 Purpose Test

The 'purpose test' identifies what the legitimate interest actually is as well as detailing the benefits for the data processing, and who will benefit.

What is the benefit of the proposed data processing? *Detail the benefits to Akrivia as well as the benefits to any other parties. You can include benefits for the wider public.*
Benefits for Akrivia The proposed processing will build Akrivia's public profile by authentically showcasing the work we do and introducing existing and prospective clients and stakeholders to key figures involved within that. It will form a critical part of our publicity and marketing strategy. An effective marketing strategy will yield commercial benefits by generating interest from both public and industry partners. **Benefits for the public** Generating interest from prospective public and industry partners will indirectly benefit the advancement of neuroscientific research given the nature of our offerings (repository of patient data, AI-driven SaaS research platform, consultancy).
How important are these benefits?
Marketing is a pilar of any business for its commercial benefits. Given the nature of Akrivia's offerings in particular, building a trustworthy and authentic public image is particularly important for promoting transparency and accountability. Producing promotional and marketing content featuring real employees feeds into that.
What would be the impact of not going ahead?
Akrivia would still be able to conduct general promotional and marketing activities. However, a publicity and marketing strategy that does not feature real employees, especially those with key responsibilities, would be one-dimensional and give the illusion that Akrivia is an unapproachable corporate entity. This is something we actively want to avoid – as above, given the nature of Akrivia's offerings, it is essential that we build a public image that speaks to our commitment to transparency and accountability. This begins with showcasing the human face of Akrivia.
What is the intended outcome for individuals?
Individuals will feature in marketing materials. Appearing in public content, such as social media campaigns, may directly or indirectly elevate their professional profile.
Are you complying with other relevant laws?

Yes.
Are you complying with industry guidelines of codes of practice?
Yes.
Are there any ethical issues with the processing? If so how are they addressed?
Fairness All requests to opt-out from the processing will be considered carefully. Where the right to withdraw and/or erase the individual's data cannot be satisfied (because overriding compelling legitimate grounds to continue), reasons will be provided to the individual. In no case will an individual suffer disadvantage for exercising their rights. **Security** Some ad hoc photo/video opportunities may arise, where individuals are photographed/recorded on colleagues' personal devices for publicity and marketing purposes on behalf of Akrivia. All personal devices used for work purposes, including these, are subject to organisational and technical measures. These include a Bring Your Own Device (BYOD) policy, a Photography SOP, and technical checks, such as to ensure that phones undergo all necessary updates and are still active. Employees are only permitted to use applications that have been approved by the Information Governance & Security Group (IGSG), including recording applications. Third party photographers, graphic designers, website developers, or other parties involved in the collection and production of promotional and marketing content featuring employees will be Akrivia's processors. They shall be subject to data processing agreements offering equivalent protection to that offered to employees by Akrivia itself, the data controller.

5 Necessity Test

The 'necessity test' examines whether the processing is necessary and whether it is necessary to rely on legitimate interests as the lawful basis for processing.

Will the processing actually help you achieve your purpose?
Given the purpose of the processing is to depict the human face of Akrivia in promotional and marketing material, images (photos and videos) are necessary for doing that.
Is the processing proportionate to the purpose?
The processing will involve taking a number of photos and videos of employees which may then be edited into social media posts, brochures, presentations, promotional videos etc. Photos and videos will also be securely stored so that they can be (re)used in subsequent materials by Akrivia.
Can you achieve your purpose without processing the data, or by processing less data?

No more photos and videos will be taken than is reasonably necessary to provide enough content for promotional and marketing material. For example, staff will not routinely be videoed or photographed in their day-to-day work.
Can you achieve your purpose by processing the data in another more obvious or less intrusive way?
It will be made clear to staff when their photo / video is being taken for marketing purposes, such as when staff attend conferences and other events intended to publicise Akrivia. Collection of the data will not happen routinely.

6 Balancing Test

The 'balancing test' balances the legitimate interest against the rights and freedoms of the data subjects. This is summed up the Jurassic Park principle – just because you can, doesn't mean you should.

6.1 The Nature of the Data

Is it special category data?
No.
Is it criminal offence data?
No.
Is it another type of data that people are likely to consider particularly 'private', for example financial data?
No.
Are you processing children's data or data relating to other vulnerable individuals?
No.
Is it data about people in their personal or professional capacity?
Yes, the character and circumstances of the images taken will reflect the individual in a professional capacity. For example, they may be photographed with other colleagues at an event where they are representing Akrivia, or they may be asked to speak about their role in the company.

6.2 Reasonable Expectations

Do you have an existing relationship with the individual? If so, what is the nature of that relationship?
Yes, employer-employee.
How have you used their data in the past?
Broadly-speaking, employee data has predominantly been / is used for necessary HR and administrative purposes. In relation to *images* of employees, save for passport photos (required under employment law and processed for entirely different purposes in different ways), images of employees have until now

been processed on the basis of consent. This includes when employees optionally upload profile photos to their various user accounts and participate in promotional and marketing activities.
Did you collect data directly from the individual?
The vast majority of the data used for HR and administrative purposes is collected directly from the employee. These images will also be collected directly from the individual by us or by our agent (processor), such as a professional photographer.
What did you tell individuals at the time?
Where images were previously taken of individuals by their consent, they were informed about such processing in our Privacy Notice and in consent forms. They were informed that they could withdraw their consent at any time.
If you obtained the data from a third party, what did they tell individuals about reuse of the data by third parties for other purposes?
Akrivia (or its processors) intend to obtain all the data from individuals directly.
How long ago was the data collected? Are there any changes in technology or other context since that time that would affect current expectations?
There is an ongoing relationship between Akrivia and its employees involving data collection. In relation to the collection and processing of *images* of employees, the only material change here is that the lawful basis relied on is being adjusted from consent to legitimate interest. This will be adjusted on Akrivia's Privacy Notice.
Is your intended purpose and method obvious or widely understood?
Taking images of employees is reasonably commonplace. Its ubiquity is in part due to the fact that including employees in promotional and marketing material is an effective marketing and publicity strategy. In this respect, our intended purpose is widely understood. It will be clear to all employees who are photographed and videoed that their images are being processed; they will not be photographed or videoed surreptitiously or in contexts they would not reasonably expect to be photographed or recorded. For example, it would be reasonable to expect that their images may be taken at events where they are representing Akrivia, such as conferences.
Are you intending to do anything new or innovative?
No.
Do you have any actual evidence about expectations, eg from market research, focus groups or other forms of consultation?
No.
Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
No.

6.3 Impact & Safeguards Risk Assessment

Risk is scored by assessing the impact and likelihood and giving a score of between 1-5. By multiplying the two scores a risk score is created between 1-25.

Impact (How bad it may be)		Likelihood (The chance it may occur)		Risk Rating					
					1	2	3	4	5
5	Catastrophic	**5**	Almost certain	5	**5**	**10**	**15**	**20**	**25**
4	Major	**4**	Likely	4	**4**	**8**	**12**	**16**	**20**
3	Moderate	**3**	Possible	3	**3**	**6**	**9**	**12**	**15**
2	Minor	**2**	Unlikely	2	**2**	**4**	**6**	**8**	**10**
1	Negligible	**1**	Rare	1	**1**	**2**	**3**	**4**	**5**

Total Risk Rating	Risk
1-3	Low
8-12	Moderate
15-25	High

Information Governance Risk Register										
		Uncontrolled Risk				Controlled Risk				
Risk Ref	**Description of Risk**	**Impact**	**Likelihood**	**Risk Score**	**Controls & Rationale**	**Impact**	**Likelihood**	**Risk Score**	**Rationale for controlled risk score & actions** *(if there are no further controls to implement, is the risk reduced and acceptable?)*	**Responsible Person**
1	Barrier to individuals exercising their rights	2	3	6	**Prior to publication** Employees will be able to exercise all applicable rights over their unpublished images. In some limited circumstances, there may be compelling legitimate grounds under Article 21(1) that override their right to object (and erase) such images. However, this is very unlikely; not following through with a request of this kind would be very likely to undermine the employee-employer working relationship. For unpublished video/audio content, the same applies as above. There may be some cases when editing the data subject's personal data out of already-recorded content will be costly or impracticable. However, in	2	2	4	Reduced, accepted	

Information Governance Risk Register										
		Uncontrolled Risk				Controlled Risk				
Risk Ref	**Description of Risk**	**Impact**	**Likelihood**	**Risk Score**	**Controls & Rationale**	**Impact**	**Likelihood**	**Risk Score**	**Rationale for controlled risk score & actions** *(if there are no further controls to implement, is the risk reduced and acceptable?)*	**Responsible Person**
					most cases this will likely be outweighed by the employee's rights and the principle of maintaining good working relationships with employees. Any determination that there are compelling legitimate grounds to continue the processing will be explained to the individual and reviewed. **Published content** Where images, videos, and audio are embedded or edited into published promotional and marketing content, it is more challenging to satisfy an objection/erasure request. The content will already be publicly available, and it may be impractical and costly to remove it. These circumstances may constitute overriding compelling legitimate grounds pursuant to UK GDPR Article 21(1), but would be evaluated on a case-by-case basis. When making this determination, Akrivia would carefully consider the employee's rights and interests and the principle of maintaining good working relationships with staff. Prior to the images being taken, it will be made suitably obvious to individuals that they are being recorded for publicity and marketing purposes, whereupon they can exercise these rights. One exception to this may be senior team leaders whose professional role can reasonably be expected to include some publicity.					
2	Barrier to individuals accessing services or opportunities	1	1	1	The processing activity will have a negligible impact on individuals accessing services or opportunities as the data relates to them in a professional capacity in a working context. As such, it has no bearing on services or opportunities they are personally entitled to. The publicity the promotional and marketing material will attract may enhance the individual's professional	1	1	1	Accepted	

Information Governance Risk Register										
		Uncontrolled Risk				Controlled Risk				
Risk Ref	**Description of Risk**	**Impact**	**Likelihood**	**Risk Score**	**Controls & Rationale**	**Impact**	**Likelihood**	**Risk Score**	**Rationale for controlled risk score & actions** *(if there are no further controls to implement, is the risk reduced and acceptable?)*	**Responsible Person**
					opportunities, although this is not the purpose of the processing by Akrivia.					
3	Loss of control over the further use of personal data due to public availability	2	5	10	Since the images will be used for promotional and marketing purposes, they, along with the individual's name and job title, will likely be made publicly available at conferences, on social media platforms, and/or in both internal and external presentations and so on. Although there are some legal protections relating to the IP of the marketing materials themselves, it would be technically and legally easy for third parties to obtain the personal data contained within for their own further uses. The combination of personal data used in the marketing materials will be limited to their professional role to limit the impact of misuse of that data. The individual may be more likely to be contacted by, or have their work email inferred by, third parties. The impact of this is relatively minor and while possible, is not guaranteed. In the event that an individual exercised their right to object, and erasure, Akrivia would endeavour to contact any known users of the images, but have no power to compel them to remove them.	2	3	6	Accepted	
4	Other losses of control over the further use of personal data	2	3	6	**Collection and storage on personal devices** Some ad hoc photo/video opportunities may arise, where individuals are photographed/recorded on colleagues' personal devices on behalf of Akrivia for publicity and marketing purposes. All personal devices used for work purposes, including these, are subject to organisational and technical measures to safeguard against loss of control. These include a Bring Your Own Device (BYOD) policy, a Photography SOP, and technical checks, such as to ensure that phones undergo all necessary updates and are still active.	2	2	4	Reduced, accepted	

Information Governance Risk Register										
		Uncontrolled Risk				Controlled Risk				
Risk Ref	**Description of Risk**	**Impact**	**Likelihood**	**Risk Score**	**Controls & Rationale**	**Impact**	**Likelihood**	**Risk Score**	**Rationale for controlled risk score & actions** *(if there are no further controls to implement, is the risk reduced and acceptable?)*	**Responsible Person**
					Employees are only permitted to use applications that have been approved by the Information Governance & Security Group (IGSG), including recording applications. **Third party processors** Third party photographers, graphic designers, website developers, or other parties involved in the collection and production of promotional and marketing content featuring employees will be Akrivia's processors. They shall be subject to data processing agreements offering equivalent protection to that offered to employees by Akrivia itself, the data controller. In all above cases, the impact is minor-moderate as the personal data involved is neither sensitive, confidential, or special category. Further uses are unlikely to cause substantial harm to the individual.					
5	Physical harm	1	1	1	The likelihood and impact of the individual being physically harmed are negligible.	1	1	1	Accepted	
6	Financial loss, identity theft or fraud	3	3	9	**Identity theft** Once publicly identifiable as working for Akrivia in a specific role, it would be possible for third parties to impersonate the individual using a fictitious work email or phone number and attempt to use it for fraudulent purposes. However, strictly enforced security protocols and training at Akrivia substantially reduce the risk of this causing a material loss to the individual (or company). For example, even if a malicious actor can infer the individual's work email, they would need to identify their password and circumvent MFA to access anything belonging to the individual or company that could be used for financial gain.	2	3	6	Reduced, accepted	

Information Governance Risk Register										
		Uncontrolled Risk				Controlled Risk				
Risk Ref	**Description of Risk**	**Impact**	**Likelihood**	**Risk Score**	**Controls & Rationale**	**Impact**	**Likelihood**	**Risk Score**	**Rationale for controlled risk score & actions** *(if there are no further controls to implement, is the risk reduced and acceptable?)*	**Responsible Person**
					Financial loss / fraud Financial loss and/or fraud would likely require malicious third parties to have the individual's bank details, personal address, and other sensitive/confidential information (a record of the individual's bank details, address etc. at Akrivia are stored completely separately and subject to stringent role-based access). Even if third parties have that data, it is unlikely that images of the individual and their job title would significantly heighten the likelihood of financial loss or fraud.					
7	Significant economic or social disadvantage (discrimination, loss of confidentiality, or reputational damage).	2	2	4	Given the marketing purposes of the processing, it is very unlikely that the individual's name, images, or job title will be associated with anything constituting reputational damage. If it did, it would reflect poorly on Akrivia, too. Before publication, all marketing materials will be quality checked to safeguard against this. The individual will not be asked to comment on anything confidential, nor will their image, name, or job title be associated with any content that could reveal confidential information about them.	2	1	2	Reduced, accepted	

7 LIA Review

View of the DPO or IG Professional. *This section is designed for the organisations DPO or appropriately senior Information Governance professional to be able to provide a qualified view of the LIA. This view should carry weight with any committees or working groups that are considering the LIA.*
The assessment makes a compelling case for the company's legitimate interest in wanting to provide a real, genuine, human face for the company in a market that is often seen by the public as faceless. The assessment notes that this cannot be achieved by sacrificing the rights of individuals. The assessment includes pragmatic steps to help safeguard individuals who do not wish their images to be captured in the first place, assurances that images are not going to be taken without the subject's awareness, and not used for additional purposes. The assessment considers the risk to the exercising of individuals' rights, particularly balancing how rights may be exercised when published, when an image is contiguous with withs (in the same picture), and video, which requires difficulty editing.

Date approved	Review by: *LIAs should be reviewed regularly and any changes documented.*
26/10/22	*David Newton*