EDENLEGAL
LAW FOR DIGITAL BUSINESS

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
<u>LIST 1: Information to be given in all cases</u> Although the information to be given is divided into two lists, with the List 2 items potentially not applicable to all processing activities, most organisations won't want multiple privacy notices for their core business so we'll end up with one covering both lists (the differences are small as we'll see, and we can draft the notice to ensure everything is covered, and in a more logical order). (What we will almost certainly will need is a second privacy notice for staff, and maybe another for candidates.)		
(1) a) the identity and the contact details of the controller and, where applicable, of the controller's representative;	Same	Self-explanatory. The representative comes into play if we are outside the EU and GDPR applies to our processing (and it will much more easily than the previous rules) e.g. because we are targeting EU customers
(1) b) the contact details of the data protection officer, where applicable;	Same	By definition this does not apply to everyone. If you don't need a DPO, consider explaining here briefly why no DPO is required – in non-obvious cases, showing that we've considered the point can be better than just glossing over it
(1) c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	Same	Both things are required here: the "purposes" and the legal bases. How granular do the purposes need to be? In theory, we should break down each purpose and obtain consent for each. However, the dividing lines are not so clear in practice – things like targeted advertising simply may not work without all their components (e.g. measurement of viewability, clicks, anti-fraud) and it may make no sense (and would potentially require pages of explanation) to allow users to choose some purposes and not others. The legal basis will often be consent, legitimate interests, or necessity for the contract – but don't make any assumptions here or hedge bets: we need to explain which one we are relying on, and make sure that we have the back up if ever challenged (so, a record of the consent action, a formal legitimate interests assessment etc. – see below).

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
N/A	(1) d) the categories of personal data concerned;	This appears only on the third party list, on the assumption that the data subject will already be aware of the categories as they are providing data directly. (Though it's good practice to set out the categories in any event.) Note that this doesn't say "data points" or "fields", but "categories". But in practice, we will want to be as detailed as we can reasonably be, especially if there is something that users might not be expecting and especially if we are processing "special categories" of data. But long lists may confuse users and make our privacy notice so long as to be unreadable in practice so, although frowned upon, some use of "such as", "including", "etc.". may be appropriate.
(1) 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;	Same	This is one that will be got wrong a lot. Using legitimate interests isn't a fall back for when we realise that we didn't obtain (or record) consent properly. It's a legal basis in its own right (and some even say preferable to consent because it implies more ongoing vigilance). If we do it correctly. And the correct way is to identify explicitly our interests and give some indication in the privacy notice of why they aren't overridden by those of our users. A balancing test (or LIA – "legitimate interests assessment") should be undertaken in every case and kept on file to show that we have properly considered both sides before selecting legitimate interests as our legal basis.
(1) e) the recipients or categories of recipients of the personal data, if any;	Same	The GDPR really doesn't say name all recipients of our data – it's possible to indicate just the categories. The WP29 Transparency Guidelines try to make the default position naming them all, but also acknowledge that just stating categories can be justified if most meaningful for the data subjects. Eden Legal would say that categories may often be easier to understand, and will make our privacy notice shorter and less subject to change. The GDPR really does say "or categories".

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
(1) f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	Same	Three points to note on this one: (1) where we used to say "your data may be transferred outside of the EEA" this won't now be enough. At least we should be saying where. And (2) how we're justifying the transfer (adequacy decision – e.g. the EU-U.S. Privacy Shield, model clauses, binding corporate rules etc. And hidden here (3) the ways that users can get their hands on them. (Actually the model clauses always said that they should be made available - in edited form - on request but here we have this as a transparency requirement in the GDPR.)

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
LIST 2: Information to be given in addition as "necessary to ensure fair and transparent processing" This information may vary depending on the circumstances or not apply at all, or only to certain data uses or certain data subjects. Even if web pages or third parties already give some of this information, Eden Legal's normal recommendation is to include as much of this as possible in our privacy notice so we know it's covered in a controlled manner.		
(2) a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;	Same	General formulations along the lines of "we retain data only for as long as necessary for the purpose collected" are still very common – but really unlikely to be sufficient (as the WP29 Transparency Guidelines specifically point out). We should be getting as explicit and granular as possible here. This may not have been given much thought and this may be a good cue to actually consider what the retention periods (or perhaps better deletion deadlines) should be. Of course they can be rolling and not fixed – so x months "from the end of the contract" or "from the last contact received from you" may work well.
(2) b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;	Same	Only the key rights stated are expressly required to be mentioned, but it must be good practice to draw attention to the others.
(2) c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;	Same	Also not in our pre-GDPR privacy notice. Copy-paste.

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
(2) d) the right to lodge a complaint with a supervisory authority;	Same	Probably good practice to say which would be the go-to authority and provide a link (except maybe in places like Germany where authorities are at state level and not national level).
(2) e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;	N/A	The key ingredient here is the consequences of not providing the data. Remembering that "not getting the service" may not be a permitted response – making a contract or service conditional upon consenting to data processing which isn't necessary for that purpose can mean that the consent is not freely given and so invalid.
	(2) f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	This clearly will only be applicable to "indirect" collections. Again, we need to make a judgment call regarding whether we need to name the source by name (more compliant) or whether a general indication of categories is sufficient (shorter and simpler).
(2) f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	Same	Not all automated decision making is created equal. Article 22 of the GDPR refers to automated decision making that has "legal or other significant effects". So what has legal or significant effects? Getting a job, a pay rise, a loan or mortgage, sure. Serving a tailored ad, probably not so much.

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
N/A	(3) The controller shall provide the information referred to [above]: 1. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; 2. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or 3. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	Our privacy notice is a really key piece of equipment in our compliance toolkit. If we are really transparent about processing then we might conceivably be able to make our consent a bit less granular. Or our legitimate interests may be easier to rely on. And complaints from users will be fewer and more easily resolved. There will be plenty of cases where we receive data from third parties. Often, our privacy notice may be the main or only way we can communicate with them where communicating directly is "impossible or would involve a disproportionate effort".

Data collected directly from data subjects:	**Data obtained from a third party:**	**Comments:**
Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to [above].	Same	OK, so where we have collected for one purpose we need to go back and inform data subjects before processing for another. Or where someone else collected the data for one purpose and passes it to us for a different purpose we need to communicate the new purpose. A new privacy notice is always an option. But for direct collections where we already have a relationship with the users, then we could potentially use an email or banner for this. Again, this is not just about validity of consent, this is provision of information for whatever legal basis we are using.