Pseudonymisation in Lamplight

Pseudonymisation in Lamplight

The GDPR applies to personal data. Pseudonymization of data is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." So pseudonymization may reduce the risks to Data Subjects and help you to protect their rights. Recital 29 of the GDPR aims to create incentives to pseudonymise data.

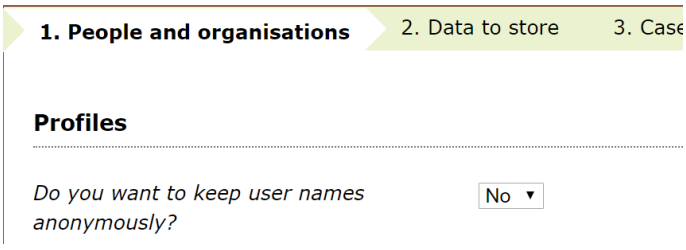
Pseudonymization is not as simple as removing names - effectively pseudonymizing it will depend on your data. For example, a date of birth and address will probably be enough to identify many Data Subjects. In some places, ethnicity and some attendance data may be enough, in others it may not be. It will depend on your data and your context.

Because judgement and context are required, there is no 'pseudonymize data' button in Lamplight. But there are some features and ways to use Lamplight that may help if you do wish to pseudonymise data.

Keep user names anonymously

You can opt to keep users anonymously if you wish to. If you do so, profiles will be referred to as 'File number 123' where 123 is their profile ID. This doesn't prevent you from adding named profiles to the system, but allows you to handle anonymous ones more easily.

To set this a system administrator will need to go to **admin > system administration > change global settings** and change the first option in the **People and organisations** tab.



As explained in the introduction, if you are omitting names you will need to ensure that other data does not readily identify the individual. You will also need to ensure your internal procedures and training are sufficient to ensure that operators do not add data that they shouldn't.

Reports

Reports in Lamplight show numbers, with in most cases no direct way to identify individuals. Publishing data from Lamplight reports may be effectively pseudonymised, but you will need to consider the following points:

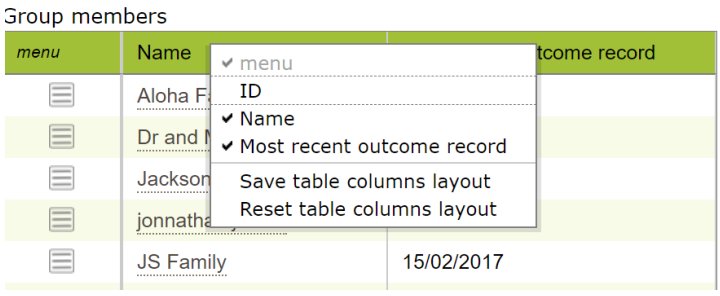
- Are there any small numbers? Breaking down report data by personal characteristics may be fine, but if there is only 1 person who is Male / Hindu in your data table they may be identifiable. You may need to aggregate smaller numbers into an 'Other' category to handle this.
- Case reports using the default settings may be identifiable, depending on how you name cases.

Reporting Access

Some operators may only require access to aggregate data that is probably reasonably well pseudonymised. For these you may wish to use the 'reporting' access level. This enables the operator to run reports, but little else, so they cannot access personally identifiable information.

Groups without names

Groups (with data views) will generally show personally identifiable information – not least names. However, you can show and hide table columns to hide names or other identifiable information by right-clicking on the table header.

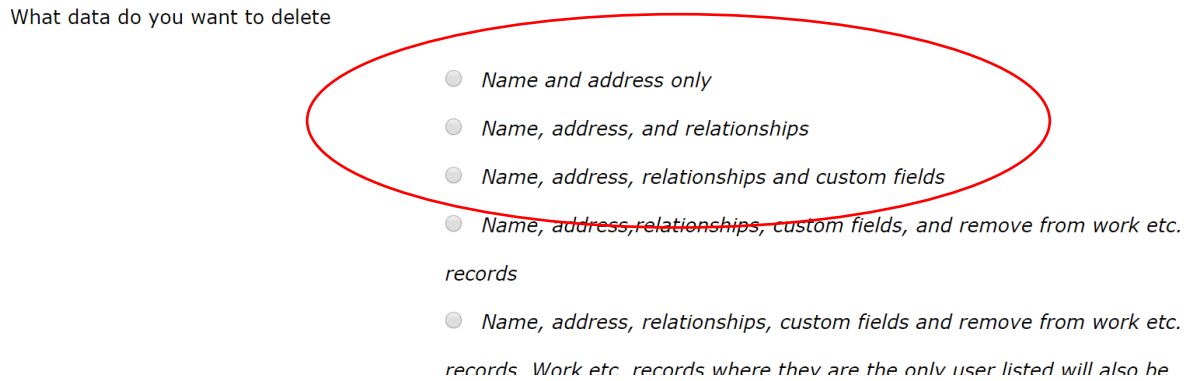


If you hide columns and then download the table, the download will not include the hidden columns.

You could also set 'Save table columns layout' with the name hidden, so that you have to take an extra step to view names. This would be unlikely to count as a sufficient measure for pseudonymisation, as it is very easy to reveal names, but could be a useful additional control in some circumstances.

Partial Permanently Delete

If you hold data for people that you wish to pseudonymise so that you can continue to run some reports on it, but no longer identify the individuals, you could partially permanently delete data. A system administrator will need to go to **admin > system administration > PERMANENTLY delete data**. Choose the profiles you wish to pseudonymise and click 'next'. On the following screen you can choose what data to delete:



Choosing one of the first three options here may be sufficient to pseudonymise the profiles selected, while leaving them as attendees of work records will allow you to run work reports.