

# **NHSmail LA webinar on GDPR question and answer log**

**17 May 2018**

Question	Answer
<p>Having read the Transparency Information, I would like clarification on the data you collect. At no time do our users submit their 'date of birth', so where is this held / collected?</p>	<p>This applies where an individual user is registering via the portal registration tool (pharmacists, optometrists, dentists, social care) – for some of those organisations, they'll need to provide their date of birth. Also, locally, organisations will need to capture any data that they collect as part of authenticating a user to receive their NHSmail account, so there may be pieces of other data that you need to include in your Transparency Information to reflect that.</p>
<p>How can we address 'Principle 5' locally in relation to the use of outlook.pst files?</p> <p><i>Principle 5: Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.</i></p>	<p>In respect of outlook.pst files, it would be a local policy decision on how long data is kept for and for what purpose. This would need to be communicated to your user base via your Transparency Information. It might be that the outlook.pst files are kept for a pre-determined period of time and deleted once this time frame expires or when the user is no longer employed, depending on the nature of the data.</p>
<p>There is no mention of the TREND portal for secure email transfer in the Transparency Information?</p>	<p>This is mentioned in the <a href="#">Data Protection Impact Assessment (DPIA)</a>. We will incorporate TREND within the Transparency Information at the next uplift in early June 2018.</p>
<p>Whilst NHS data opt-out is separate, GDPR includes the 'right to be forgotten', so surely that needs to be dealt with?</p>	<p>We have been advised that because of our legal basis for processing data, the 'right to be forgotten' isn't part of our legal position (as NHS Digital), however when you're putting together your local documentation, you'll need to consider what your legal basis is, so it may be that locally you still have to reference that.</p> <p>Further information is available on the <a href="#">ICO website</a>.</p>

Question	Answer
<p>As staff move between trusts, they will have emails from roles at other trusts which will be downloaded into our archiving system (locally). Does that mean that we become a Controller for data from other trusts, or do we become Processors for that data?</p>	<p>As Controllers, local organisations are required to implement local policies to manage the archiving of data prior to individuals leaving their organisation. This prevents data being transferred to another organisation. For example:</p> <ul style="list-style-type: none"> <li>• The organisation must ensure their data is archived out of the mailbox so it cannot be accessed by the individual once they have left the organisation.</li> <li>• Patient data must be stored in the relevant record and not in the mailbox.</li> <li>• Confirmation from the mailbox owner should be given to the Local Administrator so they can mark it as a 'leaver' prior to the account being marked as a 'joiner' within the new employing organisation.</li> </ul> <p>Should data from another organisation be retained inadvertently by the employee, the local data breach policies should enforce the action to be taken. This should take into account the guidance available within the <a href="#">Data Security and Protection Toolkit</a>:</p> <p><i>"2. Report an incident: The ability for a health or social care organisation to record and report the details of a data security and protection incident that breaches the General Data Protection Regulation / Data Protection Act 2018 to the Information Commissioner 's Office (ICO) electronically. This will also discharge the contractual and policy responsibility to report to NHS Digital, NHS England / Improvement and the Department of Health and Social Care simultaneously.</i></p> <p><i>Continued....</i></p>

Question	Answer
	<p><i>....For applicable organisations (Acute, Mental Health and Ambulance Trusts) this will allow them to report any breaches of Network and Information Services (NIS) Directive to the competent authority which is the Department of Health and Social Care. No special categories of personal data are requested.”</i></p> <p>Any data generated prior to the employee joining a new organisation remains the property of the previous organisation.</p> <p>To support this process, every user signs to accept the <a href="#">Acceptable Use Policy</a> which is being updated to reflect this approach to data management.</p>
<p>Can there be anything produced for third party organisations with locally managed accounts, and for others, that can force a requirement to re-accept the Acceptable Use Policy (AUP)?</p>	<p>There is a separate Acceptable Use Policy (AUP) that third party organisations complete when joining NHSmail. This outlines their responsibilities as an organisation as well as the AUP that individual users accept when registering their account. They will receive the broadcast communication informing them about GDPR.</p> <p>If your organisation hosts a small number of NHSmail accounts on behalf of other users, you may wish to re-enforce the AUP content via your local communication channels, as managing these accounts falls within your local policy and process.</p> <p>We’re not currently planning to force users to re-accept the AUP. Third party organisations would also fall into the remit for the local responsibilities for data management, so therefore the Joint Controller. The Joint Controller Arrangements document would clearly highlight what their responsibilities are locally.</p>

Question	Answer
<p>The timeline for processing a Subject Access Request (SAR) does not actually start until identification was been verified, not from the date of the request?</p>	<p>Requests should be managed in line with the <a href="#">ICO's Subject Access Code of Practice</a>.</p>
<p>How do we ensure that ODS data is up to date? We have a lot of organisations that have been closed but they still appear on the NHS global address list.</p>	<p>We are going to be carrying out a piece of work shortly to make sure that organisations that have legally closed are removed from the NHS Directory. We do need to make sure those organisations have removed all existing distribution lists, accounts and shared mailboxes. We can't remove the organisations from the global address list until that local activity has taken place, so we are aware there are some organisations that are still visible.</p>
<p>What about contacts data, held on the global address list, that are nhs.uk addresses from organisations that do not use nhs.net?</p>	<p>This is covered in the <a href="#">DPIA</a> and the <a href="#">Transparency Information</a> – whichever organisation has loaded those local contacts will be responsible for managing and maintaining that contact list locally.</p>
<p>Will the Transparency Information be amended to reflect the repeal of the current DPA 1998 when the UK Data Protection Bill also becomes statute on 25 May 2018?</p>	<p>Yes, we will be updating documentation once the Bill is formally passed.</p>
<p>When are we likely to see a national solution to archiving leavers' information?</p>	<p>Archiving is a local responsibility because the data falls within local remit.</p>
<p>With reference to:  <i>'Personal NHS Directory data – the information is kept indefinitely until contact details are deleted within the NHS Directory by the organisation employing the staff member'...</i>                      User accounts cannot be deleted by Local Administrators?</p>	<p>Personal data contained within the NHS Directory for non-NHSmail account holders can be deleted by the organisation employing the staff member.</p> <p>For NHSmail account holders, the Local Administrator would mark the account as a 'leaver' and, as part of the account management lifecycle, the account and any personal data contained within the NHS Directory would be deleted.</p>