

## Data Protection Impact Assessment (DPIA)

<b>Project Name:</b>	My resources – system support services
<b>Project Manager or Sponsor (PM):</b>	Vicki Richardson, Head of HR & Finance Service Centre
<b>Name of person completing the DPIA if different to (PM):</b>	
<b>Service Team and Department:</b>	Resources
<b>Relevant Director and Executive Director:</b>	Jacqueline Harris-Baker
<b>Cost Code:</b>	C13666
<b>Date DPIA received by the IMT:</b>	
<b>Date approved by DPO:</b>	
<b>Date approved by IMT :</b>	

### 1 Project Scope

*You should describe here the nature, scope, context and purpose of the processed processing.*

The Council has invested in upgrading it's ERP system to latest technology implementing the Oracle cloud solution, locally branded as My Resources which successfully went live in May 2019. "ERP" stands for enterprise resource planning. This is a suite of software used to manage finance, accounting, HR, procurement, and supply chain operations. A complete ERP suite also includes enterprise performance management, software that helps to plan, budget, predict, and report on an organization's financial results. This system is critical to the business continuity of the Council as it enables the payment of staff and suppliers, the collection of income and management of the Council's finances and employees.

Following a tender process the Council selected Evolutionary Systems Company Limited (Evosys) as it's implementation partner for Oracle Cloud

The system has been successfully implemented and went live in May 2019. The Council has an ongoing requirement, over and above what Oracle provide as part of their standard cloud services for the highest quality of support for the solution in order to ensure there is no risk to business continuity. There is a small in-house support team but at the present time the skills and capacity does

not exist in house to provide the level of technical support required to maintain the solution.

The DPIA is for a contract to provide extended support arrangements to the councils support team, for Third line support. This is the uppermost level of support in a technical support model accountable for resolving the most difficult problems. It is also known as back-end support, level 3 support, high-end support and many other titles. The title denotes expert level support for troubleshooting.

There is a significant risk to the ability of Council to operate effectively if it does not have effective support arrangements in place for it's ERP system, impacting on paying staff and suppliers, collecting income, managing the Council's accounts, managing Council employees and recruiting staff. Service failure in this area will lead to financial loss, reputational damage and impact the Council's ability to achieve statutory responsibilities.

The ongoing support services that will now be provided by Evolutionary systems company to include third line functional support to assist in the prompt resolution of system errors or bugs and configuration management. As this is a cloud solution there is a requirement to adopt quarterly upgrades and the Council requires support to understand the impact of those upgrades on it's cloud configuration and to gain an understanding of any new features that may be taken advantage of.

In addition, during the implementation of Oracle cloud a number of software tools and customisations developed by Evolutionary Systems Company Limited were deployed as part of the solutions, support for these is also needed from the supplier.

## 2 Data Description

Answer the questions below so that there is a clear understanding about how the information will be used, who will use it etc. Remember that it's personal information (i.e. information about individuals) that you need to be concerned with. If you do not have answers to all the questions at this time, simply record what you do know.

<p>Whose information is being used?</p> <ul style="list-style-type: none"> <li>- Are there additional concerns that need to be considered due to individuals sensitive/complex circumstances? i.e. vulnerable person</li> </ul>	<p>The Council's HR, payroll, finance and purchasing data. This will include data related to staff HR and payroll records. This will include Special Category Data under GDPR, which is defined as: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.</p>								
<p>What information is being used?</p> <ul style="list-style-type: none"> <li>- Consider the nature of this information E.g. Child's social care file</li> </ul>	<ul style="list-style-type: none"> <li>• Employee records</li> <li>• Financial transaction data</li> <li>• Purchase order data</li> <li>• Accounts Payable data</li> <li>• Accounts Receivable data</li> </ul> <p>Please see the below categories of Personal data that shall be processed under this agreement; this will include Special Category Data, see above.</p> <p>Description of data subjects in Oracle Cloud ERP</p> <table border="1" data-bbox="870 1360 1481 1894"> <thead> <tr> <th colspan="2">ERP</th> </tr> <tr> <th>Data Category</th> <th>Data Description</th> </tr> </thead> <tbody> <tr> <td>Suppliers and Customers</td> <td>Organisation or person Name and addresses, Email, phone numbers, contact person names and their contact details and addresses etc</td> </tr> <tr> <td>Business information of suppliers and customers</td> <td>Business type, Tax identifier, tax codes, Office or warehouse locations, Business</td> </tr> </tbody> </table>	ERP		Data Category	Data Description	Suppliers and Customers	Organisation or person Name and addresses, Email, phone numbers, contact person names and their contact details and addresses etc	Business information of suppliers and customers	Business type, Tax identifier, tax codes, Office or warehouse locations, Business
ERP									
Data Category	Data Description								
Suppliers and Customers	Organisation or person Name and addresses, Email, phone numbers, contact person names and their contact details and addresses etc								
Business information of suppliers and customers	Business type, Tax identifier, tax codes, Office or warehouse locations, Business								

# InformationMatters

Information Management Team: **Data Protection Impact Assessment**  
Version 2:0

		terms and conditions, DUNS number
	Financial details of suppliers and customers	Credit information like credit terms and conditions, bank names and bank account information
	Financial Transactions	Purchase, sales and cash transactional information with Suppliers and customers. Trade contracts, GL transactions etc
	Description of data subjects in Oracle Cloud HCM	
	Human Capital Management (HCM (HR information))	
	<b>Data Category</b>	<b>Data Description</b>
	Personal and Identity information	Employee name, Address, date of birth, national insurance number, password, visa etc
	Social	Email, contact number, job title, work history, references, interviews, disciplinary actions etc
	Financial	Bank account details, salary details, pay history
	Internal	Religious Belief, knowledge, User and password, mother's maiden name,

	Medical	Sickness absence information, medical conditions, disabilities, employee health reports
	Family	marital status,
	Behaviour	attitude, personal activities
	Sexual	Gender, sexual orientation
	Academic or education or competency	Education Qualification, Degree, year of completion, college or school attended, skills, certificates
	Employment	Job, Position, Grade, Department & Location, previous employment history, employment contracts
Does it include special category or criminal offence data?	Yes - Special Category Data	
Can an individual be identified easily from the information?	Yes	
<p>What is the potential impact on privacy of this information?</p> <ul style="list-style-type: none"> <li>- <i>What are the risks/ impact to an individual if this information was lost, stolen or manipulated?</i></li> <li>- <i>E.g. could it be sold?</i></li> </ul>	<p>There could be a significant impact on the privacy of the individuals affected if information was lost, stolen or manipulated e.g. Identity fraud from payroll information.</p> <p>Additionally there could be a significant impact if sensitive commercial information was lost, stolen or manipulated.</p>	
Will this change the manner in which we handle, use or protect this information? <i>e.g. should it be encrypted?</i>	The manner in which we handle, use or protect this information will not change, as this reflects the current processing.	


## 3 Consultation process

Consider how to consult with relevant stakeholders.

When did you consult individuals?	No direct consultation has taken place.
How did you consult individuals?	N/A
If not explain why it is not appropriate.	It is not considered necessary to consult with individuals as this project relates to delivery of technical services. However the workforce privacy statement published on the Council's information does contain information to advise that we may share information with Evosys
Who else within the organisation have you consulted with?	Procurement, legal, HR and Finance
Do you need to speak with your processor to assist?	No
Do you plan to consult information security experts or any other experts?	Consultation with the Council's ICT Security officer is ongoing.

## 4 Assessment of necessity and proportionality of data usage

<p>What is your lawful basis for processing?</p>	<p>The lawful Basis for processing will include:</p> <ul style="list-style-type: none"><li>• <b>Public task:</b> the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law. For example, the Council is required to process financial information to enable payments to be made and payments of tax etc.</li><li>• <b>Legitimate interests:</b> the processing is necessary for legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests, where this applies to processing which is not an official task.</li><li>• <b>Consent:</b> where an individual has given clear consent the processing of their personal data for a specific purpose.</li><li>• <b>Contract:</b> the processing is necessary for a contract that has been entered into with the individual, or specific steps required before entering into a contract.</li></ul>
--	---

	<p>The service has provided this table (  My Resources DPIA Lawful Basis of Proc ) which sets out the lawful basis for the processing as identified to date. This will be subject to review and revision during the term of the Contract. While the Consent and Legitimate Interests are not specifically listed in the table provided, given the range and scope of the data being processed, it is reasonable to include these, to manage the incidental processing that from time to time may take place.</p>
<p>Is consent being relied upon to share the information? Has explicit consent been obtained? Are data subjects able to opt out from giving consent?</p>	<p>No</p>
<p>Does the processing actually achieve your purpose?</p>	<p>Yes</p>
<p>How will the information be collected? (Verbally, forms, intranet, interview, 3<sup>rd</sup> party, anonymous)</p>	<p>Information entered into My resources is gathered by a variety of methods including forms, invoices, uploads and interfaces.</p>
<p>Is there another way to achieve the same outcome?</p>	<p>No</p>
<p>How will the information be used? <i>e.g. to write a report</i></p>	<p>The information will be used by Croydon Council employees as appropriate to their jobs role, e.g. finance team accessing financial information in order to manage the Council's accounts or an individual employee to book their annual leave.</p>
<p>Do the individuals know and understand how their information will be used? If there are changes to their information does the privacy notice need to be amended?</p>	<p>Yes the Council has published a workforce privacy statement on the intranet which contains sufficient reference to the sharing of data.</p>
<p>How will it be stored, kept up to date and disposed of when no longer required? <i>e.g. stored in locked cabinet/securely shredded</i></p>	<p>The information will be securely hosted, in accordance Oracle's Operational Policies, by Oracle in their Cloud Platform and will be securely disposed of after the appropriate retention period as per the corporate schedule.</p>



<p>How will you ensure data quality and data minimisation?</p>	<p>Any data changes made will be subject to agreement and quality control checking by the Council.</p>
<p>Who will have access to the information within LBC?          - <i>Include approximate number of users</i></p>	<p>All staff have access to One Oracle and will therefore have access to My Resources Oracle Cloud so around 3800. However individuals are only given access to the information that is appropriate for their job role, the security model is role based.</p> <p>One member of the support team who is responsible for supporting interfaces has access to both HCM/Payroll and Finance and Procurement. Other members of the support team and Evosys support consultants have controlled access to either HCM or Finance and Procurement.</p>
<p>Are there new or significant changes to the way we manage, use, handle or collect this information?          - <i>Include any identified concerns for the individuals, would these changes heighten risks involved</i></p>	<p>No</p>
<p>Will individuals within an existing database be subject to new or changed handling?          - <i>If yes amendments need to be made to the privacy notice and these individuals need to be informed.</i></p>	<p>No</p>
<p>What are the internal arrangements for processing this information? <i>e.g. number of staff who will have access</i></p>	<p>Access is controlled through security profiles and users are given access based on their job role.</p>
<p>How will the information be updated? <i>e.g. monthly check</i></p>	<p>Information is updated daily</p>
<p>Does the project involve the exchange of information outside of the UK and are there set standards for how the information will be treated? How will you safeguard international transfers?</p>	<p>Offshore staff at Evosys based in India will be granted access, by the Croydon My Resources Support Team, to resolve problems on a case by case basis. This access will be removed once the problem is resolved. They will be subject to the same rules on use as onshore Evosys staff.</p> <p>Croydon Council have procured Oracle Cloud technology for its back-office transformation and by default it can in</p>

	<p>theory be accessible from anywhere via internet.</p> <p>For the purpose of Oracle Cloud support, Evosys consultants will have full access to Croydon's data within the new Oracle Cloud system in order to provide the support services. Evosys offshore Consultants (India) will be accessing Croydon's data using the secure remote desktop connection which would be hosted in UK (Oracle Data's centre).</p> <p>For any activity done from offshore which shall be limited to Fault investigation, Configuration, Testing, Report and Interface Developments, the data will only be able to be viewed by individuals outside of the UK, with any operations taking place via servers based in the UK.</p> <p>The only access to data will be as a consequence of carrying out the support activities detailed within this DPIA.</p> <p>Those individuals will not be able to manipulate the data in any way. Evosys offshore Team will not be able to copy/print screen/email Croydon's data to their local machines (offshore) or to any 3<sup>rd</sup> party. Evosys offshore teams work only through a highly secure remote server based in Oracle's IAAS Data Centre in the UK. The server is further secured using McAfee's Complete Protection and Drive Encryption which restricts upload or download of data to any location other than Oracle Cloud and the clients secure FTP.</p> <p>The Evosys offshore team are employed by Evolutionary Systems Private Limited. The personal data of Evosys will therefore be transferred, for the purpose</p>
--	--

	<p>of data protection legislation, to this company established outside of the EEA.</p> <p>Data will not be accessed from any location outside of the EEA other than in India.</p>
<p>How will you prevent function creep?</p>	<p>The specification of requirements will form part of the contract and will be actively monitored through contract management arrangements.</p> <p>The scope of the support contract is listed in the schedule within the Contract. There is a change control process to approve changes to the system.</p>

## 5 Assessment of the risks to the rights and freedoms of data subjects

*You must describe the source of risk and the nature of potential impact upon individuals and identify any additional measures to mitigate those risks.*

### 5a Security

<p>Who will be responsible for the control for this information?</p>	<p>The control of information will remain with Croydon Council.</p>
<p>How will the access to this information be controlled?</p>	<p>Through creating user accounts with security profiles relevant to job role.</p>
<p>Is the data correctly managed to reduce the risk of collateral intrusion to the data subject?</p>	<p>Yes</p>
<p>Are there adequate provisions in place to protect the information? If so what are they? e.g. <i>Process, security</i></p>	<p>Access controls, secure hosting of data. A number of additional security modules, recommended by the ICT Security Officer, have been procured to provide a higher level of protection for data stored in the cloud.</p> <p>Whilst Oracle are hosting the data, the data access process will be managed by Croydon who will retain accountability for awarding of inappropriate access.</p>

	Evosys will adopt the Croydon Information Security Management System (ISMS) set of policies and guidelines.
--	---

## 5b Sharing

Who is the information shared with, why are we sharing the information with this organisation?	Data will be shared with Evosys for the purpose supporting the system												
What purpose does the information we are sharing have to the third party?  - <i>Ensure that we only share relevant information and not excessively</i>	To ensure adequate technical support is provided for the system.												
Who will have access to the information, externally?  - <i>Include approximate number of users</i> - <i>Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.</i>	<p>Evolutionary Systems Company Limited (Evosys) and Evolutionary Systems Company Private Limited.</p> <p>Evolutionary Systems Company Limited is a wholly owned subsidiary of the parent company Evolutionary Systems Private Limited.</p> <p>Please see the below details of the authorised sub processors;</p> <table border="1" style="width: 100%;"> <tr> <td>Date of Incorporation</td> <td>12-Sep-06</td> </tr> <tr> <td>Registration Address</td> <td>11th Floor, Kataria Arcade, Beside Adani Vidya Mandir School, Behind Adani CNG Pump, S.G. Highway, Makarba, Ahmedabad – 380054,</td> </tr> <tr> <td>Registration Number</td> <td>U17122GJ2006PTC049073</td> </tr> <tr> <td>ISO 27001</td> <td>Security Management</td> </tr> <tr> <td>ISO9001</td> <td>Quality Management</td> </tr> <tr> <td>Name of the company</td> <td>Evolutionary Systems Private Limited</td> </tr> </table>	Date of Incorporation	12-Sep-06	Registration Address	11th Floor, Kataria Arcade, Beside Adani Vidya Mandir School, Behind Adani CNG Pump, S.G. Highway, Makarba, Ahmedabad – 380054,	Registration Number	U17122GJ2006PTC049073	ISO 27001	Security Management	ISO9001	Quality Management	Name of the company	Evolutionary Systems Private Limited
Date of Incorporation	12-Sep-06												
Registration Address	11th Floor, Kataria Arcade, Beside Adani Vidya Mandir School, Behind Adani CNG Pump, S.G. Highway, Makarba, Ahmedabad – 380054,												
Registration Number	U17122GJ2006PTC049073												
ISO 27001	Security Management												
ISO9001	Quality Management												
Name of the company	Evolutionary Systems Private Limited												

# Information **Matters**

Information Management Team: **Data Protection Impact Assessment**  
Version 2:0

	Only staff connected directly with the support of Oracle Cloud will have access to Croydon data.
How will it be transmitted to third parties and when? How often? - <i>Provide details of software used</i>	The data will at all times be held on Servers within the UK and ESC Ltd will only be able to view the data subject to the security restrictions.
Is there a data sharing agreement in place?	Will form part of contract
At what stage will the information be transferred?	No data is being transferred

## 5c Identified Risks and assessment:

*You should take into account the sensitivity of the information and potential harm that inappropriate disclosure or use of the information could cause to any individuals concerned. You should also consider the reputational loss to the Council and the potential for financial penalties being imposed by the ICO.*

To assess the level of risk you must consider both the **likelihood** and the **severity** of any impact on individuals. A high risk could result from either a high probability of some harm or a lower possibility of serious harm.

The severity impact level and likelihood should be scored on a scale of 1 to 10 with 1 being low severity and 10 high. The two scores should be **added** together. The RAG status is derived from the following scale:

Score:

- 15 to 20 = Red (High)
- 8 to 14 = Amber (Medium)
- Below 8 = Green (Low)

### To be completed by Project Sponsor

Risk Identified	Severity of Impact	Likelihood of harm	Overall RAG rating
Inappropriate access is given to Evosys	3	2	Green
Evosys misuse access	8	2	Amber
Service provider does not comply with GDPR leading to data breaches	8	2	Amber

## 6 Identify measures put in place to reduce risk.

*You must now identify additional measures you could take to reduce or eliminate any risk identified as medium or high risk in step 5.*

### To be completed by the Project Sponsor

<b>Risk Identified</b>	<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved</b>
Inappropriate access is given to Evosys	Council controls access	Reduced	Low	Yes / No
Evosys misuse access	Council to take on Council's ISMS policies	Reduced	Low	
Service provider does not comply with GDPR leading to data breaches	Contractual obligation Contract monitoring	Reduced	Low	

## Sign off and Record sheet

Item	Name/date	Notes
Measures approved by:     Residual risks approved by:		Integrate actions back into project plan, with date and responsibility for completion.  <b>If accepting any residual high risk must consult ICO before going ahead.</b>
<p><b>Summary of DPO advice:</b></p> <p>There are a number of risks associated with the proposal, <a href="#"><u>these are summarised in the table at the bottom of this advice.</u></a></p> <p>To assist understanding of this processing I have provided the following information to place it into context.</p> <p>The Council is upgrading its Enterprise Resource Planning (ERP) system using an Oracle cloud solution (My Resources) This went live in May 2019. ERP is a suite of software used to manage finance, accounting, HR, procurement, and supply chain operations. This system is critical to the business continuity of the Council as it enables the payment of staff and suppliers, the collection of income and management of the Council's finances and employees.</p> <p>The Council has an ongoing requirement, over and above what Oracle provide as part of their standard cloud services for the highest quality of support for the solution in order to ensure there is no risk to business continuity. There is a small in-house support team but at the present time the skills and capacity does not exist in house to provide the level of technical support required to maintain the solution.</p> <p>The ongoing support services will now be supplemented by Evolutionary Systems Company Limited. As this is a cloud solution there is a requirement to adopt quarterly upgrades and the Council requires support to understand the impact of those upgrades on its cloud configuration and to gain an understanding of any new features that may be taken advantage of.</p> <p><b>Contracting Relationship</b></p> <p>Evolutionary Systems Company Limited (ESCL) is a wholly owned subsidiary of the parent company Evolutionary Systems Private Limited (ESCPL).</p> <p>The contract will be between ESCL and the Council.</p> <p><b>Processing</b></p>		



EPCPL will have access to the data in from their Head Office in India. The data will be held on servers within Oracle’s cloud platform located in the UK and the Netherlands. The data is understood not transfer ‘physically’ from these locations but EPCPL will be able to view it for the purposes of managing, providing technical support services to the My Resources Support team.

The offshore team are employed by EPCPL, the personal data it considered appropriate to treat this as ‘transfer’, for the purpose of data protection legislation, to this company established outside of the EEA.

### The proposal requires a Restricted Transfer

ICO guidance states that “...sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because they are located in a country outside the EEA; and...”

“...personal data onto a UK server which is then available through a website, and you plan or anticipate that the website may be accessed from outside the EEA, you should treat this as a restricted transfer.”

Additionally this also concerns Personal/Special Category data that is in a highly structured system/data sets relating to individuals.

The Council’s HR, payroll, finance and purchasing data. This will include sensitive data related to staff HR and payroll records as set out below:

<b>ERP</b>	
<b>Data Category</b>	<b>Data Description</b>
Suppliers and Customers	Organisation or person Name and addresses, Email, phone numbers, contact person names and their contact details and addresses etc
Business information of suppliers and customers	Business type, Tax identifier, tax codes, Office or warehouse locations, Business terms and conditions, DUNS number
Financial details of suppliers and customers	Credit information like credit terms and conditions, bank names and bank account information
Financial Transactions	Purchase, sales and cash transactional information with Suppliers and customers. Trade contracts, GL transactions etc

<b>HCM</b>	
<b>Data Category</b>	<b>Data Description</b>

Personal and Identity information	Employee name, Address, date of birth, national insurance number, password, visa etc
Social	Email, contact number, job title, work history, references, interviews, disciplinary actions etc
Financial	Bank account details, salary details, pay history
Internal	Religious Belief, knowledge, User and password, mother's maiden name,
Medical	Sickness absence information, medical conditions, disabilities, employee health reports
Family	marital status,
Behaviour	
Sexual	Gender, sexual orientation
Academic or education or competency	Education Qualification, Degree, year of completion, college or school attended, skills, certificates
Employment	Job, Position, Grade, Department & Location, previous employment history, employment contracts

## Protections Required

India is outside the EEA and EFTA and as such no current adequacy statement with GDPR exists.

Therefore any such Transfer will need to rely upon an appropriate safeguards to ensure that it is lawful. The appropriate Safeguard, in this case, would appear to be adoption of Standard Data Protection clauses issued by the ICO, with the contract. However, this may change as a result of the 'BREXIT process' and as a result of

further guidance issued by the ICO. Therefore, there is a risk that this position will need to be reconsidered in the light of events outside of the Council's control.

These appropriate safeguards are to ensure that both the Council as the Data Controller and the contractor have in place suitable controls to protect individuals' rights and freedoms in respect of their personal data.

It is noted that this proposal does not only concern staff data, it also involves business data which may include Sole Traders (who are data subjects in their own right).

The clauses contain contractual obligations that parties to the Contract are required to meet. Data Subjects are able to directly enforce those rights against the Council as the Data Controller and the For the purpose of Oracle Cloud support, EPCPL will have full access to Croydon's data within the new Oracle Cloud system in order to provide the support services, and will be accessing Croydon's data using the secure remote desktop connection which would be hosted in UK (Oracle Data's centre).

Whilst Oracle are hosting the data, the data access process will be managed by the Council who will retain accountability for awarding of inappropriate access.

For the purpose of this contract the 2010 Controller to Processor, would appear to be appropriate (this is understood to be the latest version of this clause)

On reading the standard clauses there does appears to be a requirement (4 F) to inform the data subjects of the transfer as it involves Special Category Data to a non EEA country.

However the Work Force Data Protection Policy states:

*"We require those third parties to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.*

*The council will not transfer your data to countries outside the European Economic Area."*

The processing of the data for the purposes of GDPR (and not the Transfer) would be based In this particular instance, it is likely that it would be, Public task as the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. For example, we are required to process financial information to enable payments to be made and payments of tax etc. However, this will need confirmation based upon a further details of the processing envisaged.

## Data Security Considerations


Data will not be accessed from any location outside of the EEA other than in India.


It has been stated that any activity done from offshore will be limited to Fault investigation, Configuration, Testing, Report and Interface Developments, the data will only be able to be viewed by individuals outside of the UK, with any operations taking place via servers based in the UK.

EPCPL offshore Team will not be able to copy/print screen/email Croydon's data to their local machines (offshore) or to any 3<sup>rd</sup> party. EPCPL offshore teams work only through a highly secure remote server based in Oracle's IAAS Data Centre in the UK. It is understood that the server is further secured using McAfee's Complete Protection and Drive Encryption which restricts upload or download of data to any location other than Oracle Cloud and the clients secure FTP.

It has been stated that a number of additional security modules, recommended by the ICT Security Officer, have been procured to provide a higher level of protection for data stored in the cloud. EPCPL will adopt the Croydon Information Security Management System (ISMS) set of policies and guidelines. **It was reported by the Council's ICT Business Continuity & Security Officer (at a meeting held on 17 December 2019 and email 17 December 2019) that the security issues had been reviewed and that proposed arrangements were satisfactory. A detailed note of this review is awaited and will form part of this DPIA. Further, the Audit requirement will be included within the Contracting Arrangements.**

## Risks and Issues that have been considered and addressed

Risk / Issue	Comments	Actions Required	Updates
Provide a Data 'Processing Map'	Given the issues regarding data security the proposal raises, it is important to have a clear understanding of the processing involved, by whom and the location.	Detail processing in 'Processing Map' this must include security measures.	<p><b>Processing Map</b></p>  <p>My Resources Support Process Ma</p> <p><b>provided</b></p>
Confirmation that the Council's IT Security Officer is content with the	As above and this is not clear from the DPIA as originally provided.	Need to ensure that within DPIA and related documents that there is a clear line of accountability for security and monitoring of	<p><b>This is set out in the email 17 December 2019 from the Council's ICT Business Continuity &amp; Security Officer (</b></p>

proposals.		processing etc.  These should be evidenced so that they can be included within the DPIA, along with the ICT Security Officers 'sign off'.	 RE ICO clauses amendments re sec.) provided confirmation that he is content with the proposals. Additional wording added to ICO clause Appendices 1 & 2 in the contract to cover ISO accreditation and audit.
BREXIT	Advice from ICO may change in respect of this type of transfer.	Keep under review.	Ongoing.
Lawful Basis of Processing	This is not clear from the DPIA as originally provided.	Service to provide information as to the statutory / control requirements to process the data as part of the Council's BAU activities.	Section 4 updated.
Review the Work Force Data Protection Policy regarding the processing of data outside the EEA.	The Policy is in conflict with the proposal.	(1) Liaise with Service and DPO to resolve or process data within EEA.  (2) Inform data subjects of transfer. Review the need to inform data subjects. If this not to happen record the reasons why, and any relevant	Policy updated and published on Intranet.

		mitigating actions. (see also Contracting Arrangements )	
Contracting Arrangements	<p>(1) The ICO clauses, appear to include a requirement (4 F) to inform the data subjects of the transfer as it involves Special Category Data to a non EEA country.</p> <p>(2) Need to consider contracting arrangements to provide assurance of compliance with GDPR and security of the data</p>	<p>(1) Review the need to inform data subjects.</p> <p>(2) Include within Contract: monitoring of access to 'data', Auditing of systems and work undertaken etc, and regular security reviews.</p>	<p>(1) See above.</p> <p>(2) This is set out in the email 17 December 2019 from the Council's ICT Business Continuity &amp; Security Officer; provided confirmation that he is content with the proposals. Additional wording added to ICO clause Appendices 1 &amp; 2 to cover ISO accreditation and audit.</p>
Data Minimisation	Is all the data required for the stated purpose. Would it be possible to process less data and still obtain the required results etc?	Review the data processing to ensure only the minimum data is being processed at all times.	<p>Data minimisation will be a continuous process.</p> <p>In Q1/2020 Review access to PAAS, SFTP, OTP data and Taleo.</p>

		<p>For example, does the Special Category data have to be processed in this manner?</p>	<p><b>General Principles:</b></p> <ul style="list-style-type: none"><li>• Restriction of all access to HR and Payroll access roles for Evosys consultants except for two named individuals who support HR and Payroll.</li><li>• Review scheduled jobs and ensure that appropriate accounts have been used to run the job.</li><li>• Disable any project team accounts previously used to run scheduled jobs</li><li>• To create a restricted role for Evosys consultants that can be applied by default. This access role will remove visibility and access to Personal data including special category data.</li></ul>
--	--	---	--

			<ul style="list-style-type: none"> <li>• Create a locked down admin account which is only shared with Evosys in case of emergency at the discretion of the Apps Support manager.</li> <li>• Remove access for Evosys and Project team users, to the ITSM role.</li> </ul>
Access controls and , additional security modules.	It has been stated that a number of additional security modules, recommended by the ICT Security Officer, have been procured to provide a higher level of protection for data stored in the cloud.	<p>(1) Need to evidence these as part of DPIA;</p> <p>(2) If possible reference in contract, KPI's etc; and</p> <p>(3) Undertake due diligence on contractors security, and Information Management processes.</p>	ICT Business Continuity & Security Officer. has provided confirmation that he is content with the proposals. Additional wording added to ICO clause Appendices 1 & 2 in the contract to cover ISO Accreditation and audit.
Risk Assessment	Consider risk within the DPIA as a result of ongoing review of risks and	Complete risk assessment within this DPIA prior to entering contract.	This will be kept under review and prior to completion of contact and during the term of the Contract.



	issues detailed above and within DPIA.		
<p>The above issues have been discussed with the service and the subject of review at the time of writing. As a result in view of the issues raised and the ongoing contractual work these comments are likely to be subject to revision.</p> <p>Once finalised this DPIA should be reviewed after 3 months from the agreement of the contract and then at 6 monthly intervals thereafter.</p> <p><i>(DPO should advise on compliance, measures to mitigate risk and whether processing should proceed)</i></p>			
Consultation responses reviewed by:		If your decision departs from individuals views you must explain your reasons.	
DPIA to be keep under review by:		Vicki Richardson, Head of HR & Finance Service Centre	

**If you require further guidance to complete this DPIA please contact:**

**Information Management Team (IMT)**

Ext: 47777

Email: [information.management@croydon.gov.uk](mailto:information.management@croydon.gov.uk)

**Data Protection Officer**

Email: [DPO@croydon.gov.uk](mailto:DPO@croydon.gov.uk)