22 July 2019
Our ref: 5420928

Thank you for your request received on 26 June 2019, for the following information:

1. Who is the data controller for personal data relating to payment cards?
· If it is the card provider, is there a contract in place covering this data processing?

2. Who has access to the data?
· What data protection training have these staff had?
· What organisational measures ' policies and procedures etc. - are in place to ensure that data is kept safe and not accessed by anyone without authorization?
· Please provide a copy of any written policies and procedures.

3. Have payment card users been asked to sign a privacy notice?
· What formats is the privacy notice available in?
· Please provide a copy of the privacy notice.

4. What steps have been taken to keep payment card data secure?
· What protections are in place to guard against fraud?
· How is the cardholders information (including information as to the account holder as well as any purchases) stored?
· What technical and organisational measures are in place in respect of the payment card platforms and any associated network and information systems, e.g. to prevent cyber- attacks?
· What action is taken in the event of a data breach?
· What arrangements are in place to enable access to funds in the event of a system failure?

5. Have you carried out a Data Protection Impact Assessment?

· What risks have you identified? And what mitigating action are you taking?
· If you have identified any high level risks that you are unable to mitigate what action are you taking as a result?

6. What processing operations do you actually carry out on the personal data collected?
· Who reviews the data and how often?
· Are reviews ad hoc or routine?
· If ad hoc, what triggers a review.
· Are card holders notified of a review?

7. Which organisations, if any, is this data shared with?
· Have you drawn up an Information Sharing Agreement (ISA) to govern this sharing activity?

We have processed this request under the Freedom of Information Act 2000.

Response

The council holds the information requested and it is attached/ the answers to your questions are below:

Name of your Local Authority

London Borough of Barnet

1. ***Who is the data controller for personal data relating to payment cards?***

The Council will be data controller, determining the purposes for which, and the way in which, clients' personal data is processed for the purposes of issuing a prepaid card. The provider will be the data processor processing Service Users personal data on behalf of the Council in accordance with the Council's written instructions.

- ***If it is the card provider, is there a contract in place covering this data processing?***

The Councils contractual agreement with the prepaid card provider, has GDPR compliant Controller to Processor clauses and the Council will complete the data processing schedule to set out the nature and purposes of the processing; type and category of personal data to be provided; duration of the processing; arrangements for the return/destruction of clients' personal data at the end of the processing.

2. Who has access to the data?

Service user data can be accessed, be entered or edited by designated Council and the service providers staff into prepaid card system. The following group will have access to Service User data:

- An authorised member of staff (direct payments administrator or manager, and social worker)
- Service User
- Statutory or Legal body – on request and within legal guidance
- 'Representative':
    - Who has lasting powers of attorney in relation to the person needing services.

- Who has been appointed a deputy by the Court of Protection under section 16 of the Mental Capacity Act 2005 in relation to the person requiring services.

- ***What data protection training have these staff had?***

Staff are provided with data protection training with all staff having GDPR training.

- ***What organisational measures – policies and procedures are in place to ensure that data is kept safe and not accessed by anyone without authorization?***

The prepaid card system will be accessed by Barnet Staff via an electronic token, which will give relevant Council officers access through the firewall. From there, users will need to login using an individualised username and an alphanumeric password. Council staff have been provided with training and procedural guidance on using Prepaid Financial Services' system including security protocol and keeping passwords safe. For transparency and audit purposes, the Council will maintain a user log and regularly review system access rights. The Prepaid Financial Services' system itself will log and maintain all actions undertaken by staff including logging in to the system, accessing or editing Service User data.

- ***Please provide a copy of any written policies and procedures.***

Prepaid Financial Services' system is the property of the service provider.

3. ***Havepayment card users been asked to sign a privacy notice?***

No.

- ***What formats is the privacy notice available in?***

N/A

- ***Please provide a copy of the privacy notice.***

N/A

4. ***What steps have been taken to keep payment card data secure? payments?***

In addition to the points noted above, The Prepaid Financial Services' system holding Service User data will be accessed via a secure website (password encrypted) hosted by the prepaid card provider.

The Prepaid Financial Services' system meets the following industry standard:

- Conform to all relevant Industry/Scheme Security Standards applicable to physical payment cards and include all security features required by Industry/Scheme Security Standards.
- Process and store data (including back-up data) in accordance with the Data Protection Act 2016
- PCI DSS (Payment Card Industry Data Security Standard) compliant when carrying out manual and/or automated processes.

Technical and administrative measures in place to prevent misuse of data e.g. access controls based on user responsibility and job role.

- ***What protections are in place to guard against fraud?***

To prevent internal fraud, the Council and the prepaid card provider has taken steps to put in place internal controls system controls including segregation of duties.

With regards to preventing fraud to Service Users, Prepaid card holders are provided with unique account numbers and sort codes which they need to keep safe including their password to the customer internet portal for accessing their account. This is to prevent unauthorised or fraudulent access to the user account. Should Service Users suspect their account details have been compromised, including the unauthorised or fraudulent initiation of a transaction, they can call the Prepaid Card provider or the Council to cancel the card and have a replacement card reissued. The Service User is also able to cancel or put their card on hold through the customer portal.

- ***How is the cardholders' information (including information as to the accountholder as well as any purchases) stored?***

Service user data information will be stored within the provider system for quick and easy access and retrieval. The software and the hardware that it sits on, will be hosted off site via an agreement which has been arranged by the provider.

The backup / copies process will be managed off site at and will be governed by international security standard for data storage PCI-DSS compliance which is the payment card industry security standard.

- ***What technical and organisational measures are in place in respect of the payment card platforms and any associated network and information systems, e.g. to prevent cyber-attacks?***

Service User data is currently stored in a Rackspace PCI DSS data centres, on physical servers, in two locations (both in the UK). The data is held in its own private room, with specific access rights and controls and the provider operates a full data recovery and backup policy which is tested. Rackspace's PCI DSS compliant servers adhere to the security requirements of Government, NGO and existing Council partners. Confidentiality and integrity of data-at-rest is maintained due to multiple encryption algorithms and mechanisms that are employed on the basis of security standards recommended by the PCI DSS security council and NIST and SANS Institute.

- **W *hat action is taken in the event of a data breach?***

Monthly service reviews are conducted between the provider and its sub-contractors to monitor performance and measure RackSpaces performance in hitting their SLAs and KPIs including assessing any system vulnerabilities and possible data breach. The service provider has its own data security and Business Continuity and Disaster Recovery Plan in place which has been reviewed and accepted by the Council as part of the contract arrangements.

- ***What arrangements are in place to enable access to funds in the event of a system failure?***

As noted above, the provider has put in place Business Continuity and Disaster Recovery Plan to manage such issues and the Council has aligned its own Business Continuity Plan to the providers plan to ensure efforts to recover the system are coordinated. In summary the Council will take the following broad steps in partnership with the provider:

The provider will be expected to notify the Council immediately via phone and email if their system went down, and provide regular update on progress to restoring service.

The Council will run regular weekly transaction reports in a searchable format that will enable dealing with basic transaction queries when outages occur.

Clients would be advised of other options that existed for making payments:

- Using Cash (if available)
- Allowing clients to pay for carers / services from another account and recoup the funds once portal services had resumed

The providers Customer Services will be on hand to deal with customer queries where outages occur, particularly during public *holidays and weekends.*

5. Have you carried out a Data Protection Impact Assessment?

Yes.

- ***What risks have you identified? And what mitigating action are you taking?***

The Council has undertaken a full risk assessment in undertaking its Data Protection Impact Assessment. These are currently under review and subject to further Council consideration. The risks broadly cover:

- Data Security
- Unauthorised access to systems and Service User data
- Misuse of information and data
- Data retention

- ***If you have identified any high level risks that you are unable to mitigate what action are you taking as a result?***

N/A

What processing operations do you carry out on the personal data collected?

For the purposes of supporting service users, safeguarding against financial fraud and auditing Direct Payment expenditure, the Council intends to regularly review and process Service User transactional data.

- ***Who reviews the data and how often?***

Service User transactional data will be reviewed by Direct Payment officers and also social care staff on a quarterly basis. However, reviews may be more frequent depending on the complexity of care.

- ***Are reviews ad hoc or routine?***

Routine.

- ***If ad hoc, what triggers a review.***

N/A

- **Are card holders notified of a review?**

Yes. In line with the Council's Direct Payment Policy, Service Users are formally notified of financial reviews.

1. ***Which organisations, if any, is this data shared with?***

See response to Q2.

- ***Have you drawn up an Information Sharing Agreement (ISA) to govern this sharing activity?***

This is under consideration.

If you are interested in the data that the council holds you may wish to visit Open Barnet, the council's data portal. This brings together all our published datasets and other information of interest on one searchable database for anyone, anywhere to access. http://open.barnet.gov.uk/

Advice and Assistance : Direct Marketing

If you are a company that intends to use the names and contact details of council officers (or other officers) provided in this response for direct marketing, you need to be registered with the Information Commissioner to process personal data for this purpose. You must also check that the individual (whom you wish to contact for direct marketing purposes) is not registered with one of the Preference Services to prevent Direct Marketing. If they are you must adhere to this preference.

You must also ensure you comply with the Privacy Electronic and Communications Regulations (PECR). For more information follow this Link www.ico.org.uk

For the avoidance of doubt the provision of council (and other) officer names and contact details under FOI does not give consent to receive direct marketing via any media and expressly does not constitute a 'soft opt-in' under PECR.

Your rights

If you are unhappy with the way your request for information has been handled, you can request a review within the next 40 working days by writing to the Information

Management Team at: foi@barnet.gov.uk. Or by post to Information Management Team (FOI) London Borough of Barnet, 2 Bristol Avenue, Colindale, NW9 4EW

If, having exhausted our review procedure, you remain dissatisfied with the handling of your request or complaint, you will have a right to appeal to the Information Commissioner at: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (telephone: 0303 123 1113; website www.ico.org.uk). There is no charge for making an appeal.