Information Law Solutions

Data Protection & Access to Information

Daradjeet Jagpal
5 October 2021

Outline

- Overview of data protection and access to information legislation as it applies to your role at Rosehill
- Key practical tips
- Effective risk management

Data Protection

Information Law Solutions

What is data protection?

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Regulates how Rosehill handles and uses personal data about living individuals
- Personal data
- Special category personal data
- Criminal convictions and offences personal data
- All personal data covered, including paper and electronic
- Rosehill, as controller, is responsible for compliance, but individual staff members can be held responsible for own actions

Data protection principles (DPPs)

1. Handle personal data lawfully, fairly and transparently
2. Need to specify purposes for which personal data will be used
3. Only handle and use as much personal data as needed for task at hand
4. Keep personal data accurate and up-to-date
5. Do not keep personal data for longer than necessary
6. Keep personal data secure

Transparency statement

- Identity and contact details (including DPO details)
- What personal data is going to be used for
- Legal basis for handling and using personal data
- Who personal data will be shared with
- How long personal data will be kept
- Details of individual rights and Information Commissioner's Office (ICO) contact details for complaints
- Transfers of personal data outside UK
- Consequences if not provide personal data (if provision mandatory)
- [Automated decision-making: "meaningful information" re: logic and consequences]

Data security

- Rosehill must put in place appropriate "technical" and "organisational" data security measures
- "Appropriate" depends on
  - state of art
  - costs
  - category of personal data
  - what personal data is being used for
  - risks to individuals

Data security breach

- Any circumstance in which security of personal data is compromised
- Must notify ICO of breaches within 72 hours of knowledge, if likely to give rise to risk for individuals
- If breach likely to give rise to “high risk” for individuals, then must also notify them “without undue delay”

ICO data security breach trends

	Incident Type	Total
Non-cyber security incidents	Alteration of personal data	3
	Data emailed to incorrect recipient	405
	Data of wrong data subject shown in client portal	23
	Data posted or faxed to incorrect recipient	219
	Failure to redact	95
	Failure to use bcc	62
	Incorrect disposal of hardware	1
	Incorrect disposal of paperwork	6
	Loss/theft of device containing personal data	45
	Loss/theft of paperwork or data left in insecure location	201
	Not Provided	100
	Other non-cyber incident	478
	Unauthorised access (non-cyber)	160
	Verbal disclosure of personal data	66
Cyber security incidents	Brute Force	25
	Cryptographic flaw	2
	Denial of service	1
	Hardware/software misconfiguration	45
	Malware	24
	Other cyber incident	100
	Phishing	284
	Ransomware	144
	Unauthorised access (cyber)	63

Data Range: 01/04/2021 - 30/06/2021
Quarter 1, Financial Year 2021/22

Consequences of data security breaches

- Loss of personal data
- Damage to Rosehill reputation
- Unwanted publicity
- Sued for damages by affected individuals
- Prosecution of individual Rosehill staff members involved

Managing data security breaches

- Act with urgency
- Focus on cleaning up “the mess”
- Rosehill may need to notify ICO / Scottish Housing Regulator / affected individuals / Police
- Don’t dwell on the past – learn from experience and move on

WFH data security risk management

- Use strong and secure passwords to access systems
- Do not use personal e-mail accounts / personal cloud storage accounts / personal apps for Rosehill business purposes
- Do not install unauthorised apps on Rosehill-issued devices – only use authorised apps
- Use apps for Rosehill business purposes only, not personal use

WFH data security risk management

- Secure home Wi-Fi routers using strong passwords and do not use default password (if possible)
- Do not use free public Wi-Fi, use mobile “tethering” instead
- Be aware of what and who can be seen when video conferencing
- Confidentiality of personal data at home
- Turn off and store devices safely at end of working day

Data retention

- Must not keep personal data for longer than necessary
- How determine?
  - law
  - best / sector practice
  - Rosehill business need

Individual rights

- Right to receive transparency statement
- Right of subject access
- Right to rectification
- Right to restrict
- Right to erasure
- Right to data portability
- Right to object
- Rights in relation to automated decision-making and profiling

* Age of capacity in Scotland (DPA 2018)

Engaging with service providers

- Must enter into written contract with service providers, contractors, consultants, etc.
- Contract must include provisions on
  - data security
  - confidentiality
  - restrictions on passing personal data to sub-contractors
  - assisting Rosehill with compliance e.g. rights requests

Sanctions, penalties and offences

- Individuals can complain to ICO
- ICO has range of enforcement powers, including power to issue fines of up to £17.5m against Rosehill
- Individuals can sue Rosehill for compensation for financial and non-financial damage / loss
- Offences

Effective risk management

- Keep data protection in mind when you are doing your job
- Be factual in diary entries, file notes and communications – say it like it is, don't say what you think and don't include "heat of the moment" comments
- Recognise rights requests
- Stop hoarding! Effective data retention and records management reduces rights request burden

Effective risk management

- Rights requests can cover personal e-mail accounts and SMS / WhatsApp messages and other “unofficial” communication channels used by staff for Rosehill business purposes – be careful what you say!
- Allocate sufficient time for dealing with rights requests
- Human error remains main source of data security breaches – exercise caution and “check before you send”
- Beware of risk of SHR and ICO intervention and reputational damage
- Possible HR consequences

London pharmacy fined after "careless" storage of patient data

Date **20 December 2019**
Type **News**

The Information Commissioner's Office (ICO) has fined a London-based pharmacy £275,000 for failing to ensure the security of special category data.

Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left approximately 500,000 documents in unlocked containers at the back of its premises in Edgware. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people.

Documents, some of which had not been appropriately protected against the elements and were therefore water damaged, were dated between June 2016 and June 2018. Failing to process data in a manner that ensures appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage is an infringement of the General Data Protection Regulation (GDPR).

The ICO launched its investigation into Doorstep Dispensaree after it was alerted to the insecurely stored documents by the Medicines and Healthcare Products Regulatory Agency, which was carrying out its own separate enquiry into the pharmacy.

Steve Eckersley, Director of Investigations at the ICO said:

> "The careless way Doorstep Dispensaree stored special category data failed to protect it from accidental damage or loss. This falls short of what the law expects and it falls short of what people expect."

In setting the fine, the ICO only considered the contravention from 25 May 2018, when the GDPR came into effect.

Doorstep Dispensaree has also been issued an enforcement notice due to the significance of the contraventions and ordered to improve its data protection practices within three months. Failure to do so could result in further enforcement action.

Full details of the investigation can be found in the Monetary Penalty Notice here.

Notes to Editors

Leo Kirk

Date **15 January 2020**
Type **Prosecutions**
Sector **Social care**

A former social worker has been prosecuted for passing the personal information of service users to a third party provider for Local Authority young person placements.

Leo Kirk unlawfully disclosed referrals for residential or foster placements of vulnerable young people aged 16-18 years old. The referrals contained sensitive personal data including potential identifier information and vulnerability risks of the service user.

Mr Kirk of Audenshaw, Manchester appeared before Stockport Magistrates' Court and admitted two offences of unlawfully disclosing personal data, in breach of s55 of the Data Protection Act 1998. He was fined £483 for the first offence with no separate penalty for offence two, he was ordered to pay costs of £364.08 and a victim surcharge of £48.

Google

leo kirk

All Images News Videos Shopping More Settings Tools

About 22,400,000 results (0.49 seconds)

A privacy reminder from Google

REMIND ME LATER REVIEW

www.manchestereveningnews.co.uk › ... › Denton and Audenshaw

Shamed social worker quits after being caught illegally ...

16 Jan 2020 - **Leo Kirk**, 59, had been suspended from practise for a total of 18 months by a healthcare regulator after he persuaded a grieving woman to lend ...

ico.org.uk › action-weve-taken › enforcement › leo-kirk

Leo Kirk | ICO

15 Jan 2020 - **Leo Kirk** unlawfully disclosed referrals for residential or foster placements of vulnerable young people aged 16-18 years old. The referrals ...

dentoncorrespondent.co.uk › tag=leo-kirk-tameside

Leo Kirk Tameside – Denton Correspondent

28 Jan 2020 - By Sophie Wheeler A SHAMED social worker has quit after he was caught illegally sharing confidential and highly sensitive information on ...

www.facebook.com › public › Leo-Kirk

Leo Kirk Profiles | Facebook

View the profiles of people named **Leo Kirk**. Join Facebook to connect with **Leo Kirk** and others you may know. Facebook gives people the power to share and...

socialworktutor.com › leo-kirk-social-worker-took-money-from-vuln...

Social worker took money from vulnerable woman to pay his ...

22 Apr 2019 - **Leo Kirk**, a social worker who was contracted to Warrington Borough Council, helped a service user win her £4,800 benefits appeal, then asked ...

www.warringtonguardian.co.uk › news › 16164303.warrington-boro...

Warrington Borough Council social worker Leo Kirk ...

17 Apr 2018 - Warrington Borough Council social worker **Leo Kirk** suspended by Health and Care Professions Council. By Adam Everett Reporter.

popstar.one › news › persons › leo-kirk

geese rescued after diesel spillage in city centre canal
to all British passport holders
fans as 'creepy' character sexually attracted to son
looks amazing as she reveals her weight loss
as Manchester house 'starts to collapse'

Shamed social worker quits after being caught illegally sharing confidential and highly-sensitive information on troubled children

He was banned from frontline duties at the time

By **Sophie Wheeler** & **Amanda Crook**
09:58, 16 JAN 2020

NEWS

MOST READ

1

Martin Lewis' warning to all British passport holders

2

Ex Corrie star Sarah Lancashire horrifies fans as 'creepy' character sexually attracted to her 15 year old son

3

'Forget Adele' - Real Housewives star looks amazing as she reveals her

Access to Information

Information Law Solutions

Access to information: introduction

- The “right to know” has existed in Scotland since 1 January 2005
- Freedom of Information (Scotland) Act 2002 (FOISA) = access to information (applied to Rosehill since November 2019)
- Environmental Information (Scotland) Regulations 2004 (EISRs) = access to environmental information (applied to Rosehill since June 2014)

FOISA: information covered

- Covers information re: “housing services”
  - prevention and alleviation of homelessness
  - management of housing accommodation, but only where Rosehill granted SST or short SST (does not cover information about factoring activities)
  - provision and management of sites for gypsies and travellers, whatever their race or origin
- Also covers supply of information by Rosehill to SHR re: financial wellbeing and governance standards

EISRs: information covered

- Covers information on

a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;

b) factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in paragraph (a);

c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in paragraphs (a) and (b) as well as measures or activities designed to protect those elements….

Key features

- Right of access to information / environmental information held BUT it is not a right to *re-use* accessed information / environmental information
- Publication schemes (FOISA) / active dissemination (EISRs)
- Records management
- Fees
- Exemptions (FOISA) / exceptions (EISRs)
- Codes of practice
  - handling requests
  - records management
- Scottish Information Commissioner (SIC)

Requests

- FOISA: writing or other “permanent form”, which is capable of being used for subsequent reference
  - voicemail
  - recorded telephone calls
  - social media e.g. Twitter direct message
  - Internet requests e.g. sent via https://www.whatdotheyknow.com/
- EISRs: verbal requests are sufficient
- Name of applicant and address
- Information / environmental information want access to
- [Preference re: how to be provided]

Who can make a request

- Requester is known as “applicant”
- Anyone, anywhere in the world
- No requirement to have interest or any connection to Rosehill
- Age of capacity: 12+ but could be lower

Duty to advise and assist

- Rosehill must provide reasonable advice and assistance to applicants and prospective applicants

Duty to transfer request (EISRs only)

- If Rosehill does not hold requested environmental information, but believes another Scottish public authority holds some or all of it, Rosehill must either
  - transfer request to other authority, or
  - provide applicant with name and address of other authority to allow applicant to make request to it

Fees

- Optional – no need to charge
- Different charging schemes for published and unpublished information / environmental information
  - published = costs of providing
  - unpublished = costs of locating, retrieving and providing
- Maximum FOISA fee = £50
- Maximum EISRs fee = unlimited (but must be reasonable)
- Issue a fees notice
- Fees notice must be paid within 3 months (FOISA) or 60 working days (EISRs) – otherwise, request lapses

Response deadline

- Respond “promptly” and in maximum of 20 working days (EISRs: can extend by additional 20 working days due to volume and complexity of requested environmental information)
- Clock starts when valid request received by any member of Rosehill staff
- Clock pauses once fees notice issued until paid
- Routine amendments to information / environmental information can be made while processing request

Responding to requests

1. Comply with request and disclose information / environmental information
2. Do not hold requested information / environmental information
3. Repeat request (EISRs: “manifestly unreasonable” request)
4. Vexatious request (EISRs: “manifestly unreasonable” request)
5. Refuse request and exempt some or all information / environmental information

- In all cases, include
  - details of review process (review within 40 working days of response)
  - right to make application to SIC (apply within 6 months of review)

Enforcement and offences

- SIC
  - information / decision / enforcement notice
  - appeal to Court of Session
- Offence
  - alter, deface, erase, destroy or conceal record after request been received with intention of preventing disclosure, unless Rosehill would not have had to provide the information / environmental information to applicant
  - Fine of up to £5,000 for Rosehill and any staff member involved

Effective risk management

- Ensure requests appropriately handled and routed, with prompt responses
- Issue robust and detailed responses, bespoke to each request
- Maintain audit trails – record progress of request, parties consulted and decisions taken
- Ensure requests for review are meaningful
- Use out of office notifications
- Remember personal e-mail accounts and SMS are not outwith scope
- Publish as much as possible

Contact

Daradjeet Jagpal
Director and Legal Consultant
T: 00 44 7852 905 779
E: daradjeet@infolawsolutions.co.uk
W: www.infolawsolutions.co.uk
@infolawsol

Information Law Solutions