Greene King Data Protection Policy

Version 1

27th July 2018

Contents

Purpose

This policy sets out Greene King's rules for the processing and protection of personal data and electronic communications data. Adherence to this policy will help Greene King comply with data protection law and manage the risks to data subject and the commercial risks to the business which arise from Greene King's processing activities.

Scope

This policy applies to the processing of personal data and electronic communications data by or on behalf of Greene King. This policy is supplemented by other policies and guidelines, which provide more detailed information on specific topics. These currently include:

- Information security policy set
- Subject access policy
- CCTV Policy
- Group Retention Schedule
- Standard data processing agreement for data processor contracts
- Data protection impact assessment guidelines
- Marketer's guide to using guest data
- Guide to using personal data in IT systems during testing

Further specialised policies (such as a policy for taking photos and recording video and audio footage of people) will be issued over the course of the next year. If you cannot find the policy or guidance you require, ask the data protection officer for assistance.

Intended Audience

Audience	Relevance
Greene King directors	For **action**. You are **accountable** for the processing activities which take place within your division, business unit or function, or which you have sponsored. You must ensure that adequate control measures are implemented to manage these processing activities in compliance with this policy. You must also ensure that any risks which arise from these processing activities are managed in accordance with Greene King's risk appetite position.
Greene King managers	For **action**. You are **responsible** for the processing activities which take place within your business area. You must ensure that adequate control measures are maintained, effective and monitored and that any out-of-tolerance processing-related risks are remediated.
Greene King employees, contractors, team members and agency workers	For **information**. You are **responsible** for ensuring that you follow Greene King's processing procedures, which are derived from the control objectives found within this document, by your management team. This document will be helpful to you if you want to understand the rationale for these procedures. Ask your manager for more information about the processing procedures you are required to follow.

Audience	Relevance
Organisations processing data on behalf of Greene King	For **information**. You are **responsible** for ensuring that your organisation complies with this policy in respect of the processing your organisation carries out on behalf of Greene King.

Table 1 Intended audience and relevance

Mandatory control objectives are set out in part 4 and the control records required to evidence the existence and effectiveness of your control environment are covered in Part 5. Part 6 provides information about individual role accountabilities and responsibilities.

Definitions

Term	Definition
Data subject	An identifiable living person that personal data relates to.
Electronic communications data	Any text, voice, sound or image message sent over a public communications network (e.g. the internet, telephone lines, mobile telephone masts) which can be stored in the network or on the recipient's equipment (smartphone, tablet, laptop, PC, etc.). Electronic communications data may or may not also be personal data.
Greene King	All legal entities, divisions, business units, functions, operations, teams and staff of the Greene King group of companies.
ICO	The Information Commissioner's Office. The ICO is the UK's data protection authority (or 'supervisory authority' in GDPR), responsible for enforcing data protection law within the UK.
Personal data	Any information that identifies or relates to a data subject, when processed alone or in combination with other personal data.
Personal data incident	An undesirable, unexpected or unplanned event involving personal data.
Personal data breach	A personal data incident which poses a risk to data subjects.
Processing	Any activity that involves or affects personal data or electronic communications data, including (but not limited to) collection, storage, use, disclosure, transfer, amendment or deletion.
Sensitive data	Data which a data subject is likely to think of as being especially confidential e.g. special category data, financial information, private correspondence .
Special category data	Personal data that relates to a data subject's: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where they are being used to identify someone), health, sex life or sexual orientation. Special category data are subject to additional rules and safeguards under GDPR, as is criminal offence data.

Table 2 Definitions

Status

This policy is effective from 27th July 2018 and will remain in force until it is updated or replaced. This policy will be reviewed before the start of each calendar year.

Part 1 Legal Context

The EU General Data Protection Regulation ('GDPR') and UK Data Protection Act 2018 ('DPA') both came into force in May 2018, bringing with them some very significant changes to the law governing personal data processing.

General Data Protection Regulation

GDPR provides data subjects with an enhanced set of rights intended to enable them to retain control over the use of their personal data. Whilst most of these rights are not new, they have been increased in potency and made much easier to exercise, resulting in a shift in the balance of power away from data controllers and towards data subjects.

As well as empowering data subjects, GDPR imposes new obligations on data controllers, such as the requirement to be able to provide evidence of compliance when asked to do so by a regulator, and the requirement to report all impactful personal data breaches to a regulator within 72 hours of becoming aware of an incident. Controllers are also required to directly notify data subjects of any incidents which are likely to seriously affect them.

GDPR also provides regulators with enhanced powers to help them enforce the regulation. The financial sanctions which regulators can impose on data controllers have increased significantly and they are also able to direct or curtail a controller's processing activities.

Data Protection Act 2018

The new DPA is a companion law to the GDPR. It sets out the alterations, exemptions and clarifications that the UK government has decided to make to GDPR using powers the regulation confers on EU member state governments for this purpose. Importantly, the DPA also sets out how GDPR will be applied once the UK has left the European Union and further increases the powers of the UK regulator, the ICO. The Act also creates some new offences and brings the EU Law Enforcement Directive into UK law.

Privacy and Electronic Communications (EC Directive) Regulations 2003

Whilst GDPR and DPA have become the primary UK data protection laws, the Privacy and Electronic Communications (EU Directive) Regulations 2003 ('PECR') remain in force. PECR regulates data processing in the context of electronic communications and applies to all communications data, whether personal or not.

PECR often applies in addition to GDPR and DPA. Amongst other things, PECR sets out very specific rules for electronic direct marketing communications, processing location data via public telecommunications networks and interacting with user's devices.

Whilst PECR were not updated in May, the effect of these regulations has altered because they rely in part on concepts which have been redefined by GDPR, such as the new definition of consent and the new requirement to retain evidence to prove the validity of consent. PECR will themselves be updated once the proposed EU ePrivacy Regulation is finalised. This is likely to be the case even if the UK has by then left the European Union.

Other Laws and Standards

Depending on the nature of a processing activity, other laws, obligations or standards may also need to be considered, such as:

- The Equality Act 2010
- UK health and safety law
- UK licensing law
- The laws of another country when processing takes place in another jurisdiction
- The Advertising Standards Authority's Code of Non-broadcast Advertising and Direct & Promotional Marketing (CAP Code)
- The Payment Card Industry Data Security Standard (PCI DSS)

This collection of laws and standards presents us with a vast, comprehensive but complex regulatory framework. Greene King is issuing this new data protection policy to provide a simple and concise set of principles and control objectives for governing Greene King's processing activities which will help ensure compliance with the law.

Part 2 Governance Model

Data Governance Committee

The Greene King data governance committee is responsible for establishing and maintaining Greene King's data protection policy and for ensuring the business operates in compliance with it.

The data governance committee is chaired by the chief financial officer and the primary business leads are the company secretary and IT director. If you want to bring something to the attention of the data governance committee, including requests for modifications, exemptions or exceptions to this policy, contact the company secretary first.

If the data governance committee is unable to make a decision on a matter, they will escalate it to the operations board.

Data Protection Officer

Greene King has appointed a data protection officer ('DPO') to provide independent advice on all matters relating to privacy and data protection. You can contact the DPO on 07812 257475 or by email at dataprotection@greeneking.co.uk.

Compliance with this policy will be assessed by the DPO, supported by Greene King's audit teams. The DPO's findings will be reported to the data governance committee, operations board and audit and risk committee.

Contact with the ICO, including the notification of personal data breaches, is managed by the DPO.

Part 3 Processing Lifecycle

Greene King has defined a simple, four-phase processing lifecycle to help determine when to apply data protection control measures. The lifecycle phases are used to provide context in subsequent sections of this policy. The table below describes each phase of the lifecycle:

Phase	Description	Risk Focus	Control Focus
Prepare	The Prepare phase involves planning, analysis and risk assessment activities, especially for risks to the rights and freedoms of data subjects. A key goal of the Prepare phase is to ensure that data protection is applied by design and by default throughout subsequent phases of the lifecycle by identifying which control measures must be in situ to manage the risks which arise from the processing.	Identify, Assess	Design
Get	The Get phase involves accessing and acquiring pre-existing personal data, and computing, deriving or otherwise creating any new personal data. This is the phase in which processing commences, therefore security and compliance risks must be managed from this phase onwards.	Manage, Remediate	Implement, Monitor, Assess
Use	The Use phase puts the remainder of the controls identified during the Prepare phase into operation, to protect the data obtained during the Get phase. During the Use phase, all data protection measures must be continuously monitored so that any movement in risk or undesirable incidents which may occur are detected and managed appropriately.	Manage, Remediate	Monitor, Assess
Dispose	The Dispose phase involves anonymising or securely destroying any personal data which are no longer required for processing. Disposal is triggered in line with the Group Retention Schedule and is carried out in compliance with the Information Security Policy Set.	Manage, Remediate, Close	Monitor, Assess, Withdraw

Table 3 Processing lifecycle

Part 4 Processing Principles and Control Objectives

Greene King's processing activities must be carried out in accordance with certain principles: to successfully apply those principles, a set of control objectives must be met. These principles and accompanying control objectives are described in the table below:

Principle	Control objectives
Lawfulness, fairness and transparency	1. Processing activities must have a valid lawful basis. 2. Data subjects must be informed about the processing. 3. Processing activities must conform to the description of them provided to data subjects. 4. Data subjects must be informed of and able to exercise their rights. 5. Personal data must not be disclosed, shared or transferred without a valid justification. 6. The need for additional control measures must be evaluated whenever processing is likely to carry a high risk for data subjects.
Purpose limitation	7. Processing must be necessary to achieve a clearly defined purpose. 8. If personal data are to be processed for a new purpose, the conditions for lawfulness, fairness and transparency must be met first.
Data minimisation	9. Processing must involve the minimum necessary number of personal data and data subjects. 10. Processing must continue for no longer than is necessary. 11. Processing may occur no more frequently than is necessary.
Accuracy	12. Personal data must be accurate enough to enable the purpose of the processing to be achieved. 13. Inaccurate personal data must either be rectified before they are processed, or deleted.
Storage limitation	14. Personal data must be disposed of when no longer needed. 15. Personal data may only be disposed of by securely deleting or anonymising them.
Security	16. The confidentiality, availability and integrity of personal data must be maintained at all times.
Accountability	17. Control measures must be implemented to meet these control objectives and to manage risks to data subjects and risks to the business. 18. Risks must be managed within defined tolerances. 19. Control measures must be monitored and assessed, for adequacy and effectiveness. 20. Any control deficiencies which are identified must be remediated promptly. 21. Control monitoring, assessment and remediation activity and associated findings must be documented. 22. Data incidents must be notified to the data protection officer, data protection authority and data subjects, as appropriate.
Data protection by design and by default	23. Processing activities, risks and control measures must be designed, tested and documented before processing commences.

Part 5 describes the records which need to be kept to evidence the adequacy and effectiveness of the processing control environment.

Part 5 Control Records

Certain records must be kept in order to implement the control objectives set out in Part 4, and track their adequacy and effectiveness. These records are shown in the product breakdown below:

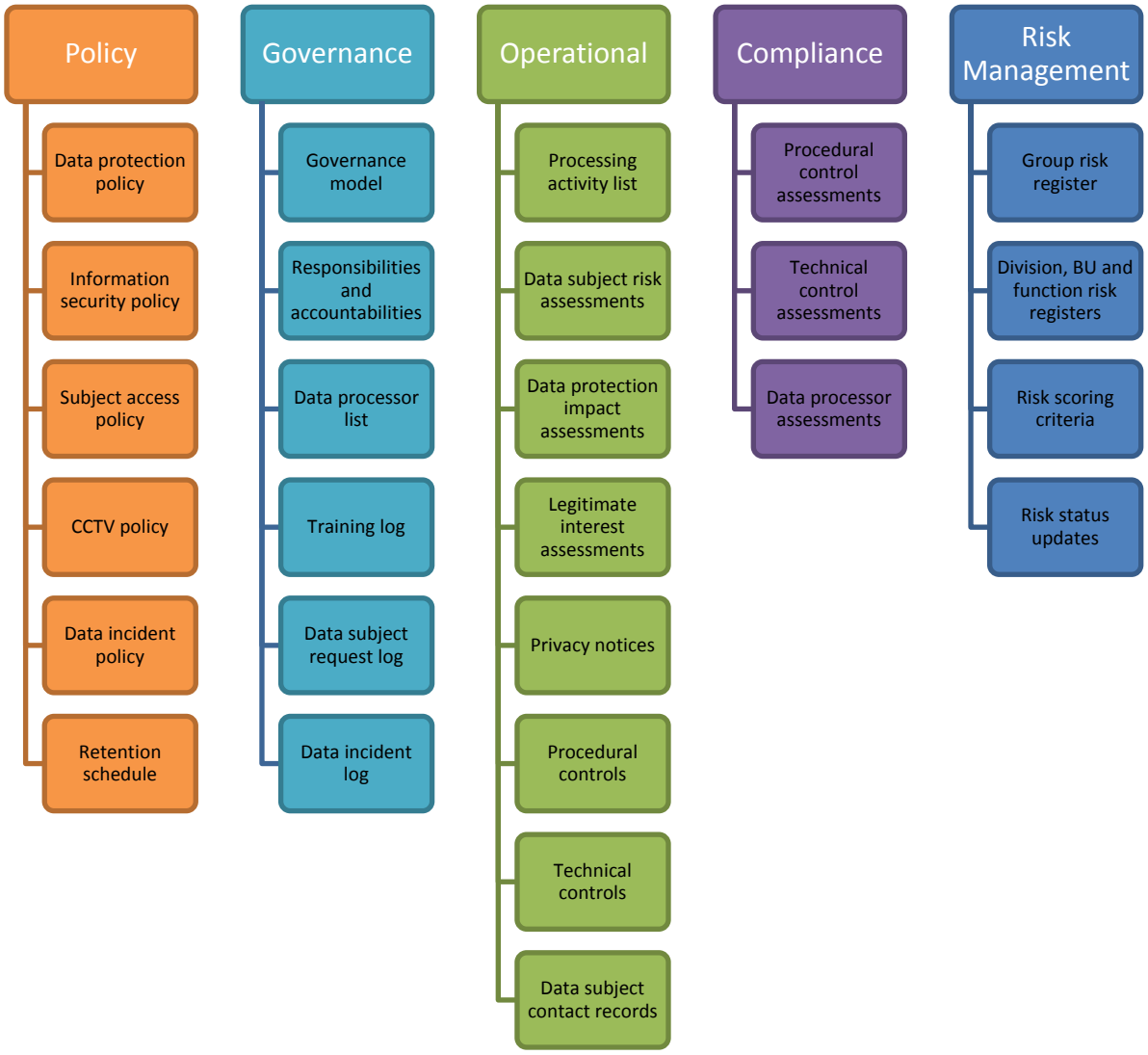

Figure 1 Control records product breakdown

Part 6 sets out who is accountable and responsible for the elements which make up the processing control environment.

Part 6 Accountabilities and Responsibilities

In order to achieve the control objectives described in Part 4 and produce the control records described in Part 5, certain activities must be carried out. The following table lists these activities in column 1 and shows the accountable and responsible role-holders for each activity in columns 2 and 3 respectively:

Activity	Accountable	Responsible
Maintain the data protection policy	Company Secretary	Data Protection Officer
Maintain the Information security policy set	IT Director	Infrastructure Manager
Maintain the subject access policy	Company Secretary	Data Protection Officer
Maintain the CCTV policy	Company Secretary	Security and Safety Manager
Maintain the data incident policy	Company Secretary	Data Protection Officer
Maintain the group retention schedule	Company Secretary	Data Protection Officer
Operate the data protection governance model	Data Governance Committee	Data Protection Officer
Assign data protection accountabilities and responsibilities	Data Governance Committee	Data Protection Officer
Maintain the data processor list	Relevant directors	Relevant managers
Maintain the data protection training log	Learning and Development Director	Learning and Development Manager
Maintain the data subject request log	Company Secretary	Data Protection Officer
Maintain the data incident log	Relevant directors	Relevant managers
Maintain the processing activity list	Relevant directors	Relevant managers
Conduct data subject risk assessments	Relevant directors	Relevant managers
Conduct data protection impact assessments	Relevant directors	Relevant managers
Conduct legitimate interest assessments	Relevant directors	Relevant managers
Implement, maintain, monitor and assess processing principle control measures (see Part 4)	Relevant directors	Relevant managers
Provide privacy notices	Relevant directors	Relevant managers
Maintain data subject contact records	Relevant directors	Relevant managers
Conduct control self-assessments	Relevant directors	Relevant managers
Conduct independent control assessments	Company Secretary	Data Protection Officer
Conduct data processor assessments	Relevant directors	Relevant managers
Set risk scoring criteria	Company Secretary	Head of Risk
Maintain the group risk register	Company Secretary	Head of Risk
Maintain division, BU and function risk registers	Relevant directors	Relevant managers
Provide risk status updates	Relevant directors	Relevant managers

Table 4 Accountability and responsibility matrix

These activities must provide evidence of the design adequacy and effectiveness of the control measures and therefore demonstrate that there is adequate control of the processing activities.

Part 7 Data Protection by Design

This part of the policy brings together all of the previous parts by providing a planning checklist for new processing activities.

New Processing Activities

Step 1 Identify which personal data must be processed, by what means, to achieve the purpose.

Step 2 Identify a valid lawful basis for each processing activity.

Step 3 Determine whether or not any other organisations will be involved in the processing. If they will, identify the control measures that will be required to legitimise, monitor and assess their processing activities.

Step 4 Conduct a data subject risk assessment (DSRA) to identify any risks to data subjects that may arise from the processing.

Step 5 If the DSRA indicates a likelihood of a high risk to data subjects, complete a data protection impact assessment (DPIA). Use the findings of the DPIA to determine what preventive, detective and corrective control measures are necessary to manage the risks to data subjects within an acceptable tolerance range.

Step 6 Determine what personal data records will be created as a consequence of the processing activities and how long these should be kept for. Include audit trail, compliance and evidential records in this step.

Step 7 Once all planning activities are complete, request conditional approval for the processing from the DPO.

Step 8 Once conditional approval has been granted, document the processing activities and their associated control measures.

Step 9 Draft the privacy notice.

Step 10 Train those who will be involved in the processing to: carry out the processing; recognise and respond to data protection-related enquires from data subjects; monitor and manage risks to data subjects; recognise and escalate data incidents.

Step 11 Request approval to commence the processing from the DPO.

Step 12 Once approval has been granted, implement the control measures, publish the privacy notice and commence the processing.

Step 13 Once processing is underway, commence the control monitoring and assessment activities

Step 14 Notify any data incidents to the DPO as soon as they arise.

Approved Processing Activities

Refer to the processing activity list to see which processing activities have been approved. If a processing activity is not included in the list but you think it should be, inform your manager or the DPO.