Legal and Contractual Requirements Policy
(includes intellectual property)

Objective and Scope

The objective of this policy is to document how Prevision Research manages its legal, statutory, regulatory and contractual obligations related to information security business and IS systems to mitigate risk of data, personal information or contract breaches.

The scope of this procedure is limited to legislation related to aspects of information and cyber security, the protection of personal information and business contractual information.

Roles, Responsibilities and Authorities

The Operations Director takes responsibility for identification of legislation pertinent to privacy of personal information and for maintaining compliance to such legislation.

The Operations Director takes responsibility for identification of legislation pertinent to contractual obligations and for maintaining compliance to such legislation.

The Operations Director takes responsibility for identification of legislation pertinent to cyber security and for maintaining compliance to such legislation.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction
Online Safety Act 2023	https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
The Copyright, Designs and Patents Act 1988	https://copyrightservice.co.uk/
National Assistance Act 1948	https://www.legislation.gov.uk/ukpga/Geo6/11-12/29/enacted
The Freedom of Information Act 2000	https://www.legislation.gov.uk/ukpga/2018/12/contents

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Interested parties	4.2			
Compliance with legal and contractual requirements		18.1.1		5.31

Legal and Contractual Requirements Policy
(includes intellectual property)

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID
Intellectual Property rights		18.1.2		5.32

Related Information

- Legal and Regulatory (Data Security and Privacy) Register
- Change Management Procedure

Policy

Identification of applicable legal requirements

Applicable legal requirements shall be identified across the scope of the organisation's activities. This includes global and regional jurisdictional considerations for legislative obligations in relation to information and cyber security and the protection of personal information of individual persons.

A Legal and Regulatory (Data Security and Privacy) Register shall be maintained and contain, as a minimum:

- List of legislation and/or regulations and/or Article or Code reference relating to any obligation in relation to cyber security, information / data security or privacy of personal information
- Legal/regulatory document name e.g. General Data Protection Regulation EU (GDPR) / UK
- Jurisdiction covered by the legislation such as country, state or region
- Authority enacting the applicable legislation
- Registration requirements - are you required to register with the authority?
- Obligation to provide a competent person to oversee the legislative obligations
- Scope of the legislation as it relates to data collection, processing and transfer of personal information
- Data security obligations as it applies to the scope of company activities
- Breach notification obligations as it applies to the scope of company activities

Assignment of responsibilities to develop and maintain the register sits with the relevant information technology (for cyber security) or privacy officers (for personal information).

The register shall be reviewed annually and also when known changes to legislation or business operations occur, including additional services or operational jurisdictions expansion.

Identification of applicable contractual requirements

Identification of applicable contractual requirements is the domain of senior management with legal knowledge to:

- Identify and manage contract law obligations including intellectual property rights

Legal and Contractual Requirements Policy
(includes intellectual property)

- Enter into legal agreements to deliver services and provide products within the business operations in relation to information / data security, personal information protection and intellectual property rights
- Provide terms and conditions commensurate with fair trading

Contractual agreements shall be authorised by a management representative.

Cryptography - see also Cryptography Policy

Cryptographic laws fall into four main categories:

- Import controls, which is the restriction on using certain types of cryptography within a country.
- Export control, which is the restriction on export of cryptography methods within a country to other countries or commercial entities.
- Patent issues, which deal with the use of cryptography tools that are patented.
- Search and seizure issues, on whether and under what circumstances, a person can be compelled to decrypt data files or reveal an encryption key.

Jurisdictional laws within the ISMS operational scope must be known and observed including those laws that enforce access to encrypted information by a regulatory body. This will influence when encryption can be used. The Operations Director must agree to the intended encryption use.

Intellectual property rights

Copyright

Intellectual property rights at Prevision Research is addressed, taking into consideration:

- the ownership and management of intellectual property developed by the company in the course of business activities
- the rights of intellectual property of those products and copyright material that are used in the course of business.

Prevision Research senior management shall maintain a list of intellectual property and copyright licences including databases, designed computer programs and other materials: Software List

The copyright licence and mark is displayed on all associated materials distributed by the company.

Use of proprietary software applications

Prevision Research uses proprietary software under license (copyright) user agreements that declare limits of use, distribution and modification imposed by the product owner. Software applications and user agreements are held in a list/register by the Operations Director and montoried to ensure the end -use agreement defined conditions are not breached.

Policy review

Legal and Contractual Requirements Policy
(includes intellectual property)

This policy shall be reviewed under the technical review obligations of ISO 27001 by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N