POLICY/PROCEDURE: DATA PROTECTION POLICY

TITLE: DATA PROTECTION POLICY

INDEX:

1.0 INTRODUCTION

Thyson Technology Ltd needs to gather and use certain information about individuals. This can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

This Policy should be read in conjunction with:

- Thyson's Information Security Policy (TTLPol016)
- Thyson's Network Security Policy (TTLPol018)
- Thyson's Access Control Policy (TTLPol017)

2.0 WHY THIS POLICY EXISTS

This data protection policy ensures Thyson Technology Ltd:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

3.0 DATA PROTECTION LAW

Both the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018 replacing the Data Protection Act 1998. The DPA 2018 applies GDPR standards but it has been amended to adjust those that would not work in the national context. It also has a part that transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the GDPR and Part 3 of the DPA 2018 sets out the requirements for the processing of personal data for criminal 'law enforcement purposes'.

The regulations describe how organisations — including Thyson Technology Ltd — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. The regulations are underpinned by six important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Be processed in a manner that ensures appropriate security of the personal data.

4.0 PEOPLE, RISKS AND RESPONSIBILITIES

4.1 Policy scope

This policy applies to:

- The head office of Thyson Technology Ltd
- All branches of Thyson Technology Ltd
- All staff and volunteers of Thyson Technology Ltd
- All contractors, suppliers and other people working on behalf of Thyson Technology Ltd

It applies to any information that the company holds and processes that relate to a natural person who could be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, metal, economic, cultural or social identity of the natural person.

Sensitive personal data is a specific set of "special categories" that must be treated with extra security including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; the processing of genetic data, biometric data (where processed to uniquely identify someone), data concerning health or sexual orientation.

Sensitive personal data should be held separately from other personal data, preferably in a locked drawer or filing cabinet. As with personal data generally, it should only be kept on laptops or portable devices if the file has been encrypted and/or pseudonymised. Organisation require explicit consent from the individual to processing sensitive personal data.

4.2 Data protection risks

This policy helps to protect Thyson Technology Ltd from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

4.3 Responsibilities

Everyone who works for or with Thyson Technology Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and the policies referred to in Section (2) and the data protection principles. Failure to do so may be subject to disciplinary action.

Given size and data processing activities of Thyson Technology Ltd it is not required to appoint a Data Protection Officer. However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Thyson Technology Ltd meets its legal obligations**.**

- The **Financial Director** is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Maintain the Thyson Data Security Incident Register
  - Dealing with requests from individuals to see the data Thyson Technology Ltd holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.

5.0 GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those **who need it for their work.**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Thyson Technology Ltd will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular**, strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

6.0 DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.** For more information see Information Security Policy (TTLPro016) section 6.11.4.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location,** away from general office space.
- All data back-ups are stored on a Synology NAS device located in the Server room, for more information see Business Continuity Plan (TTLPro060).
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

7.0 DATA USE

Personal data is of no value to Thyson Technology Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal **data should not be shared informally.** In particular, it should never be sent by email, as this form of communication is not secure.
- Data must **be encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be **transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

8.0 DATA ACCURACY

The law requires Thyson Technology Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Thyson Technology Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held **in as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Thyson Technology Ltd will make it **easy for data subjects to update the information** Thyson Technology Ltd holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

9.0 SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Thyson Technology Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations.**

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at mailto:finance@thyson.com. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

10.0 DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Thyson Technology Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

11.0 PROVIDING INFORMATION

Thyson Technology Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request.]

12.0 PERSONAL DATA BREACH PROCEDURE

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

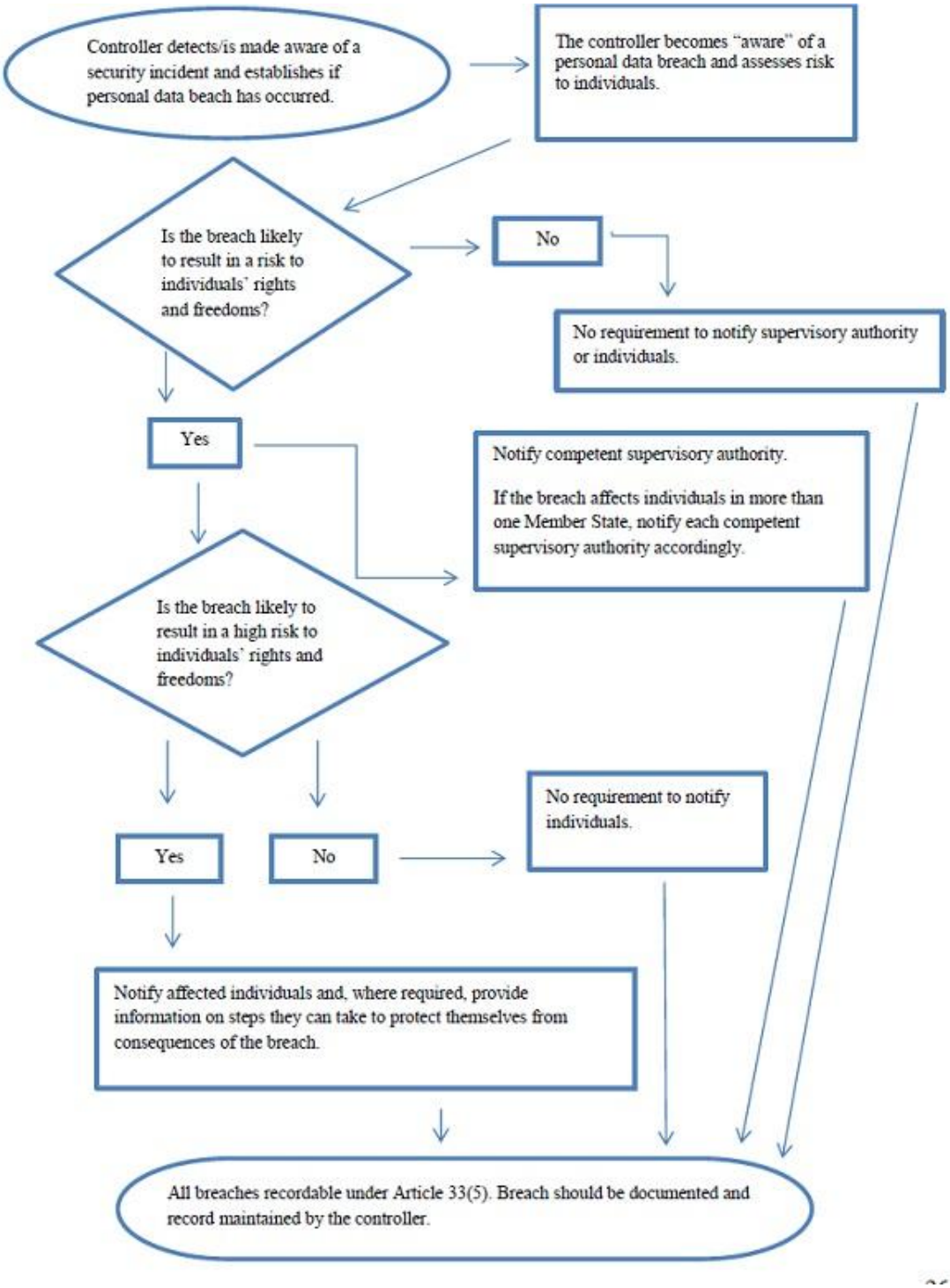
Any such events, including events that may potentially lead to a data security breach, must be reported to the Finance Director within 24 hours. Failure to do so may be subject to disciplinary action. All reported

incidents will be recorded on the Thyson Data Security Incident Register that will be maintained by the Finance Director.

The Finance Director will notify the relevant supervisory authority of a breach if it is likely to result in a risk to the rights and freedoms of individuals i.e. may result in discrimination, damage to reputation, financial loss or loss of confidentiality or any other significant economic or social disadvantage.

The Thyson Data Breach Procedure is included in Appendix A.

Appendix A: Data Breach Procedure



Appendix B: Privacy statement

When you request information from Thyson Technology Ltd, sign up to any of our services or buy things from us, Thyson Technology Ltd obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the Data Protection Act to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

We would also like to contact you in future to tell you about other services we provide, and ways in which you might like to support Thyson Technology Ltd. You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

Very occasionally we carry out a joint mailing with carefully selected other organisations, in order to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, either ask for an application form to be sent to you, or write to the Data Protection Officer at Thyson Technology Ltd. There is a charge of £10 for a copy of your data (as permitted by law. We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

For the web site, additional information is usually included. This would cover:

- Does the web site collect IP addresses, and if so does it link them to the individual in order to track their future visits?
- Does the web site set any cookies, and if so what are they used for?

Appendix C: Confidentiality statement for staff and volunteers

When working for Thyson Technology Ltd, you will often need to have access to confidential information which may include, for example:

Personal information about individuals who are supporters or otherwise involved in the activities organised by Thyson Technology Ltd.

Information about the internal business of Thyson Technology Ltd.

Personal information about colleagues working for Thyson Technology Ltd.

Thyson Technology Ltd is committed to keeping this information confidential, in order to protect people and Thyson Technology Ltd itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Thyson Technology Ltd to be made public. Passing information between an agent and the UK office, or between Thyson Technology Ltd and a mailing house, or vice versa does not count as making it public, but passing information to another organisation does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information between the UK office and agents;
- not gossip about confidential information, either with colleagues or people outside Thyson Technology Ltd;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Thyson Technology Ltd.