Data Protection Policy

The aim of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections, e.g. by the client within the scope of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance.

Introduction

Paye Solutions Ltd. (Registered in England & Wales 4635602) is the limited company which processes payroll for and on behalf of client companies throughout the UK. As a core part of what we do Paye Solutions Ltd receives and holds the personal information for and on behalf of companies and their employees. This data is needed to provide a compliant payroll service. At no time is this data used for any other purposes other than that which is specified in our Service Contract.

Security policy and responsibilities in the company

We consider it imperative that we hold all data in a secure way at all times.

- This means that we will use the latest technology, where possible, to secure data; and ensure that our processes do not unnecessarily risk exposure to any unauthorised third party.
- We will update our policies, processes and technology regularly to achieve the safest possible data security.
- We will train our team to understand the risks of handling and processing data.

Legal framework in the company

- We have a lawful reason to hold and process data
- We will ensure that our policies meet the most recent legislative requirements
- We will follow the laws within the UK

Existing technical and organisational measures (TOM)

- We have compliant servers to back up data and email accounts on exchange servers with Microsoft office 365. They are ISO/IEC27002 and ISO/IEC27001 compliant.
- We also require regular network and application testing to ensure the security of our systems and our client's data.
- Our Privacy Policy provides further documentation on the use of data that we hold.

In addition to the above:

- We require password protection on all computers
- We educate all of our team on the proper use and secure handling of data
- All applications and data are backed-up every 24 hours to our cloud provider Acronis which is UK based.
- We run regular application protection protocols to protect against malware
- We have a specialist third-party provider that monitors our applications, servers and hosting facility to ensure that we are secure and compliant.

We are open and transparent to our clients about our efforts to protect data. We also remind our clients that they should always transfer data to us in a secure manner. Clients should password protect documents before sending them to us.

If our clients choose alternative methods of sharing information with us, we will remind them that they are not following best practice in safe handling of employee data.
At all times, we encourage our clients to be mindful of taking due care when sharing or requesting any sensitive employee information.