Functionality and Development

being carried out and implemented for the addition of a

Payroll & HR

Data Management Tool (DMT)

assisting our clients in their journey to GDPR compliance

Item		Note		Date requested
PRODUCT:		Profile Enterprise		
CHANGE REQUIRED:		Various function changes/updates		
CLIENTS:		All		
DOC VERSION:		V4.0		
Author:		Les Bichard		
Date Created:		28.11.2017		
Latest Revision:		232/05/2018		

Contents

Section 1: GDPR Explained

The General Data Protection Regulation (GDPR) is likely to impact smaller companies. A recent study shows that 82% of SMEs are still unaware of how to interpret the new legislation and although there is expected a period of grace where if you are shown to be putting GDPR functions in place, there is the potential to be hit with large fines after May 25th 2018.

The GDPR will replace all the existing data protection laws across Europe and shape the way in which companies handle, protect and profit from data. All businesses and not-for-profit organisations that process personal data concerning employees, customers or prospects who are in the EU and/or are EU citizens fall within its scope, wherever in the world the company is based and even if the data is processed outside the EU.

In other words, European data protection law will now apply worldwide, and businesses have until 25th May 2018 to prepare.

Sigma have been proactive in preparing our Profile Enterprise Payroll & HR Suite ready for the GDPR commitments.

Through GDPR, the EU recognises:

1. The right to private life as a universal human right

   and

2. The right to have one's personal data safeguarded as a distinct, standalone universal human right

It is by attaching rights to an individual's data separately to the right attached to an individual, that the EU can demand EU-grade data protection standards on businesses in other countries. The onus is on businesses to determine if they are in scope. Consider three simple questions:

1. Is your organisation based in the EU?
2. Does your organisation handle data regarding EU-based individuals?
3. Does your organisation do any kind of business with organisations to which 1 or 2 apply?

If you answered yes to any of the three questions, it is most likely that your organisation is in scope of the GDPR. Unless you are confident your existing data handling procedures are already compliant with the regulation, this means action needs to be taken now to prepare for the May 2018 deadline.

There has been a lot of noise in the IT press about swingeing fines and GDPR is frequently portrayed as the new corporate bogeyman. It has to be said these fears are not without foundation: a two-tier sanctions regime will apply and breaches of the law could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs.

However, scaremongering is not a constructive approach. The good news is that correct implementation of the GDPR will not only ensure compliance and mitigate the risk of fines but, more importantly, will give compliant businesses a competitive advantage. That's why Sigma advocates that organisations consider GDPR a central base of business strategy that has high visibility with the Board.

Section 2: A 12-step plan to assist you through the process.

1. **Brief senior management**

   Ensure the board is aware of the changes to data protection law and how this affects the business.

Kick-off a GDPR programme

This should be led by C-level executives (or heads of department in smaller organisations) and include the CEO, CIO, CSO, CCO. MD or whoever is responsible for Compliance. The importance of having IT and Legal people speaking the same language and briefing the Executive cannot be stressed enough.

Consider whether your organisation needs to appoint a DPO

The GDPR requires public authorities and other organisations whose core activities require regular and systematic monitoring of data subjects on a large scale, or that process a large scale of special categories of data to appoint a Data Protection Officer (DPO) who will guide the implementation of GDPR requirements and monitor compliance. The DPO should be the head of the data privacy governance structure, liaise with appropriate supervisory authority(s) and report directly to leadership. The ideal candidate will be IT conversant, and have good business acumen whilst also being proficient on all GDPR matters. Recruiting a DPO may prove time-consuming, so we advise customers to make this a priority.

Update data governance policies and procedures

to ensure they reflect the GDPR requirements.

Analyse the GDPR and understand the legal implications for your business

Identify the risks associated with your business model and address them by means of adequate data governance. Where appropriate, streamline processes. Pay attention to processes that use personal data for profiling. Marketing, HR and Sales will probably need to adjust their ways of working to ensure compliance.

Review your Record Management Strategy

Identify where personal data is being collected or acquired, the purpose for which it is being processed, and whether this data is shared with any other organisation. If this information is not currently available, a detailed investigation will be required so that all personal data and its flow within the organisation is accurately mapped.

Run an awareness campaign in your company

Unless your business is a one-man band, you need to ensure that all personnel are aware and engaged in the quest for GDPR compliance.

Challenge the basis under which personal data is stored, collected and processed

Review the more prescriptive GDPR definition of consent and determine if a new request for consent is necessary.

Implement any necessary technical adjustments to ensure GDPR data rights are fulfilled

These are the right to be informed, to rectification, to erasure, to restrict processing, to object and rights in relation to automated decision-making and profiling and the new right to data portability.

Review the current mechanisms for international data transfers EU-US

Be aware that the adequacy of Privacy Shield (which replaced Safe Harbour) is currently a subject of concern.

Examine your supply chain

Ensure your efforts to comply are not undermined by engaging in business with non-compliant providers or business partners.

Embed privacy in your operation

This is the only sustainable way to ensure compliance on an ongoing basis. GDPR is here and will be for the foreseeable future, even after Brexit.

Section 3: The main areas of GDPR that will impact HR

According to Weightmans LLP, the areas of GDPR that will impact HR are as follows:

1. Consent
2. Data rights
3. Subject access rights
4. Breach reporting

1. Gaining consent to process employee data

When you want to do something with somebody's personal data, you need to gain their consent. When GDPR arrives, the rules on gaining this consent will change. Previously, consent could be gained by writing in a "consent to process data" clause into a contract. But under GDPR, consent must be "freely given, specific, informed, and clearly indicated".

The good news for HR, is that this does not necessarily apply to employee data. This is because, according to Sue Lingard of Cezanne HR, you can instead rely on an "other lawful basis" in order to process employee data. Or in other words, you are processing the data because it is a legal requirement for you to do so.

Be warned that any employee data you store or process for reasons that fall outside of your legal obligations, will still require the new, more explicit consent GDPR will introduce.

New rights for employees as data subjects

Employees will have more rights over what happens to their personal data. Law firm Taylor Wessin, breaks down all employee data rights under GDPR into a handy six-point summary:

a) **The right to be informed.** You must be clear to your employees exactly how you use their personal data

b) **The right of access.** Subject Access Requests will still exist, but with different rules, under GDPR

c) **The right to data rectification.** If employee data is wrong, or key data is missing, the employee may request this is corrected. This isn't much different to existing data protection legislation

d) **The right to be forgotten.** Taylor Wessing is quick to point out that this only applies to employee data under certain circumstances

e) **The right to block or suppress personal data processing.** Again, this is very similar to existing legislation

f) **The right to data portability.** This is brand new under GDPR. Employees may now obtain their personal data, and reuse it for their own purposes, across different services. This is another situational right, so won't always apply

As you can see, a lot of employee rights as data subjects are the same under GDPR as they are under existing DPA legislation. But there are new rights that did not exist before, and some rights have changed a little.

Subject access rights

Under the DPA legislation, data subjects had the right to request all information you held on them and you were allowed to charge a nominal fee of £10 for your trouble.

Subject access requests are not going anywhere. Previously, you were obliged to fulfil the request within 40 days. But under GDPR, you must now fulfil requests 'without undue delay', and within one month or 4 weeks depending on your processing jurisdiction. You may no longer charge a fee, either – unless requests are deemed to be excessive.

Luckily for employers, if a subject access request is particularly complex, you may extend the time it will take you to comply, according to Clare Gilroy-Scott, writing on PersonnelToday.com:

"This will be able to be extended by up to two additional months by informing the employee within one month of the request of the need for the extension, and the reasons why."

Breach reporting

Anybody involved in the processing of personal data within your organisation, must now follow a new breach reporting process. This includes payroll & HR departments.

If there is a breach of any personal data, GDPR requires you to notify the Information Commissioner **within 72 hours** if possible. If this is not possible, you must also provide justification as to why it wasn't possible.

A personal data breach could be anything from a lost laptop, to an email sent to the wrong address. But it's worth noting that these kinds of mistakes won't always be classed as a personal data breach – you only need to report a breach that is likely to result in a risk to a data subject. For example, if you lose a laptop which stores unencrypted employee records.

Section 4: How do we see the Sigma payroll products and HR software being affected by GDPR:

Sigma provide the vessel to store, monitor and report on data and have created a small module that will assist the client. This Data Management System (DMS) module will be available in the latest version of Profile Enterprise. (V443 & Above)

With this in mind these are the three suites of products that we currently support which facilitate the storage or allow the processing of employee data

a) Sigma Pay Payroll

It is not intended to add any GDPR functionality to this product and all clients will be offered the opportunity to upgrade to the Profile Enterprise Suite

b) Profile SBE Payroll & HR

It is not intended to add any GDPR functionality to this product and all clients will be offered the opportunity to upgrade to the Profile Enterprise Suite

c) Profile Enterprise Suite

1. Profile Enterprise Payroll (Integrated with HR)
2. Profile Enterprise HR (Integrated with the payroll)
3. Profile Intranet (Self-Service)
4. Profile Learning & Development Module

The premise of the changes we are to make will be to clearly have distinct division between the Payroll and HR data elements and give the users opportunity to set how long they need to keep specific data.

E.G. Payroll Data could be set for 10 years But HR data could be 7 years etc.

GDPR data retention brings with it several potential problems when keeping/removing employee data.

- Once data has been removed the client needs to be informed when making any employee enquiry relating to the now deleted employee data
- When a request for a reference is received the ex-employee may have worked for you for many years but there could no longer be any information held about them within the system
- If Payroll Data is deleted but there is still HR data and Vice versa, the employer would need to be informed of that data deletion had taken place

All data deletions will be shown to the client prior to deletion if the client requires.

Section 5: What will be required:

The system will be altered to take GDPR requirements in account for all of our clients' needs and this includes the following areas

a) Payroll Data retention
b) HR Data retention
c) Employee Data sheets
d) Deleting Data
e) Auditing
f) Searching

We will have options to:

1. **Set Payroll data retention period**

This is a configurable option set on each **Division** screen to allow the client to enter a period range of data to keep (E.G. 3 years 04 months)

This will also have a selection for the employee statuses that are to be deleted. It is possible that the client may need to delete data only for Ceased or Applicant Employee types whilst keeping the Current employee's data until they become ceased. At that stage their data would become deleted according to the settings in the system

Create routines to delete Payroll data prior to data retention date

There will be two options to allow this to happen

Option 1: Manual selection to remove data. This will have a screen which shows when the data has been cleared to when the routine was last run

Option 2: This will be an automated routine whereby there is no interaction required by the user and data is automatically deleted when the system is open however, this deletion must be reported to a log file or screen accessible by the user for checking prior to deletion

Set HR data retention period

This is a configurable option set on the **Division** screen (E.G. 7 years 0 months)

This will also have a selection for the employee statuses that are to be deleted. It is possible that the client may need to delete data only for Ceased or Applicant Employee types whilst keeping the Current and Archived employee's data, until they become ceased. At that stage their data would become deleted according to the settings in the system

Create routines to delete HR data prior to data retention date

There will be two options to allow this to happen

Option 1: Manual selection to remove data. This will have a screen which shows when the data has been cleared to and when the routine was last run

Option 2: This will be an automated routine whereby there is no interaction required by the user and data is automatically deleted when the system is open however, this deletion must be reported to a log file accessible by the user for checking prior to deletion

To generate a data sheet on each employee for agreement to keep their records

A report will be available that details all information that is recorded about the employee. There are three sections to this

Section 1: Details of data that is required to hold the employees HR details

Section 2: Details of data that is required to pay the employee

Section 3: Details of data that does not fit in the above criteria I.E. you may wish to pay death in service benefit to the next of kin, so you will have a legitimate reason to hold that particular bit of data

This report will be available in such a format that the Employee can agree and sign for what data can be held regarding section 3 above

Ability to delete all of the Payroll Data for Individuals

This option will be available on a screen with appropriate security. This routine would be able to completely delete all information regarding an individual for any date range if they are an applicant or ceased or archived

This will also include Audit trail information

However, within the database we will have an option to store the following information if required:

1. Work No
2. First name
3. Surname
4. Date deleted
5. Reason for dilation

The above fields will be kept encrypted within the database. This will allow us to use minimal reporting on previously deleted data. This is useful if you receive a request to prepare a reference for a deleted employee without identifying the individual. This allows you to search on the items above (1 to 4) and report back that you no longer have the data within your system

Full Audit Trail details to be removed

Data deletion means that the data will be removed from the database permanently

The data will be deleted from the following areas.

- Database tables relating to the Employees record
- Internal Audit screens
- We will report on **the Network paths** of where documents reside, relating to each deleted employee that are stored within Enterprise. The employer will then have a printed list of the relevant document(s) on their network that are linked to Profile Enterprise, that they may wish to manually delete

IMPORTANT NOTE: The client will also need to give thought to **previous data backups** and **documents** not recorded within profile Enterprise as they may hold data that you also need to delete

SAR (Subject Access Requests)

There will undoubtably be SAR requests from employees in the future and these need to be handled efficiently and in a timely manner. To assist our clients, we are adding a SAR tracking button.

When a SAR is received, the client can start the timer and this will count down the days you have available to comply. At a later date, this module will also be able to email your team at certain user-defined milestones.

Disclaimer:

Data Management Tools

The data input, recorded and held within the Profile Enterprise suite of products and the validity and retention of that data is solely the responsibility of the clients own appointed DPO for policies and the clients own appointed Data Controllers

Sigma have provided certain tools and routines described in this document as Data Management Tools (DMT. Provision of the DMT will not, in any manner, implied or otherwise, make your business GDPR compliant but are made available to assist the client in their own processes towards GDPR compliance

There is no obligation to use the DMT if you wish or are able to put other processes in place

It is solely the responsibility of the client, to ensure the validity of any data the system stores, generates, reports on and deletes when using the DMT.

SAR Reports

Sigma have made every effort to report on the data held within Profile Enterprise for the individual selected.

We have supplied criteria and the areas of data you can report on and each client can select the areas that are required for the SAR Reporting.

It is solely the responsibility of the client, to ensure the validity of any data the system stores, generates and reports on when using the SAR Report.

The report is built as a PDF but can be exported to Excel if required.

End -----

E&OE