simplisys

GDPR Compliance Toolkit

Version 1
Date: 12th December 2017

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk
www.simplisys.co.uk

Contents

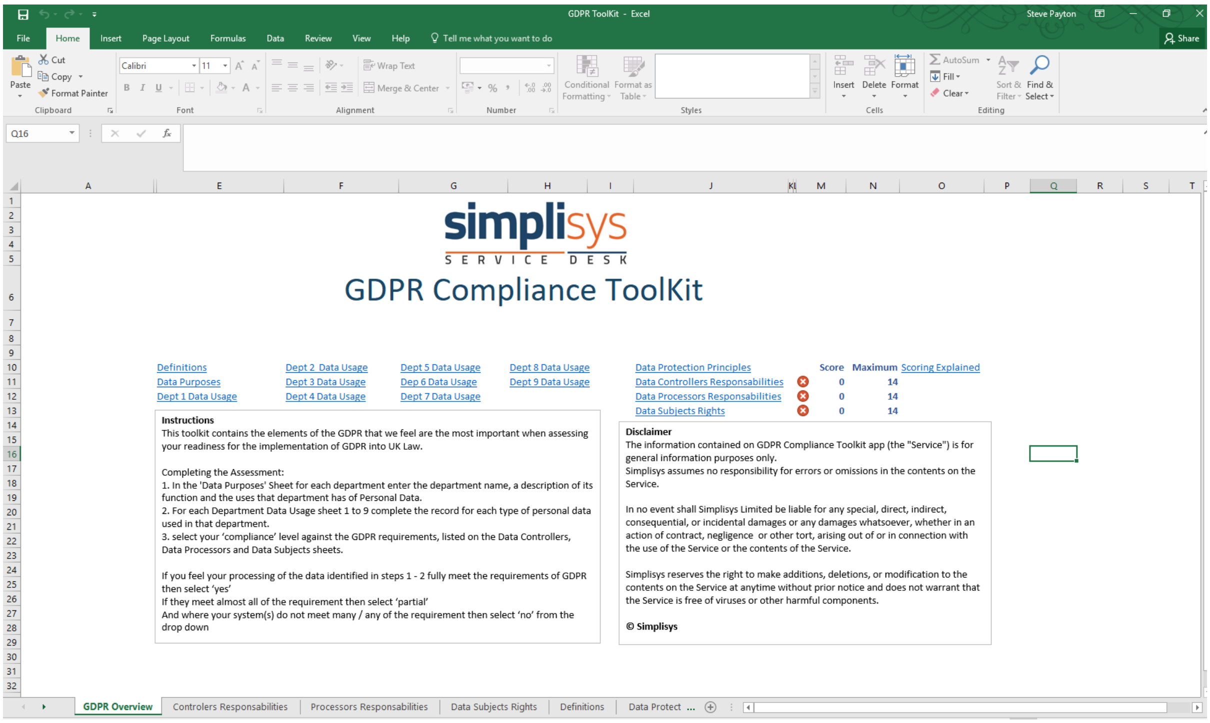
Overview

This toolkit contains the elements of the GDPR that we feel are the most important when assessing your readiness for the implementation of GDPR into UK Law.

The toolkit takes you through the steps of identifying the Personal data being processed, identifying the reasons for processing the data and finally identifying your compliance with the GDPR.

The Toolkit

The toolkit is driven from the 'GDPR Overview' tab. From here you can select a hyper link to take you to the section of the toolkit you are working on and see an overview of your compliance status.



GDPR Compliance ToolKit

Definitions
Data Purposes
Dept 1 Data Usage
Dept 2 Data Usage
Dept 3 Data Usage
Dept 4 Data Usage
Dept 5 Data Usage
Dep 6 Data Usage
Dept 7 Data Usage
Dept 8 Data Usage
Dept 9 Data Usage

Data Protection Principles		Score	Maximum	Scoring Explained
Data Controllers Responsabilities	☒	0	14	
Data Processors Responsabilities	☒	0	14	
Data Subjects Rights	☒	0	14	

Instructions
This toolkit contains the elements of the GDPR that we feel are the most important when assessing your readiness for the implementation of GDPR into UK Law.

Completing the Assessment:
1. In the 'Data Purposes' Sheet for each department enter the department name, a description of its function and the uses that department has of Personal Data.
2. For each Department Data Usage sheet 1 to 9 complete the record for each type of personal data used in that department.
3. select your 'compliance' level against the GDPR requirements, listed on the Data Controllers, Data Processors and Data Subjects sheets.

If you feel your processing of the data identified in steps 1 - 2 fully meet the requirements of GDPR then select 'yes'
If they meet almost all of the requirement then select 'partial'
And where your system(s) do not meet many / any of the requirement then select 'no' from the drop down

Disclaimer
The information contained on GDPR Compliance Toolkit app (the "Service") is for general information purposes only.
Simplisys assumes no responsibility for errors or omissions in the contents on the Service.

In no event shall Simplisys Limited be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with the use of the Service or the contents of the Service.

Simplisys reserves the right to make additions, deletions, or modification to the contents on the Service at anytime without prior notice and does not warrant that the Service is free of viruses or other harmful components.

© Simplisys

Compliance Scoring

The scoring mechanism is designed to show how compliant you are to the core GDPR requirements in the three areas:

1. Data Controllers Responsibilities
2. Data Processor Responsibilities
3. Data Subjects Rights

After you have identified personal data processed in your organisation using the Data Purposes and Data Usage sheets you should consider how compliant your organisation is against each of the requirements in each of the three areas above.

To indicate you are compliant for a given requirement select 'Yes', if you are almost fully compliant select 'Partial' otherwise select 'No'

You compliance in each area is assessed and a visual indication, along with a score, given on the the 'GDPR Overview' tab.

To get a Green indication ● you will have to be compliant for each requirement in the section

If you have a single area where you are partially compliant, but all the other requirements in that section are met then you will get a amber indicator.

If you have more than one 'partial' in a section you will get a red ● or red cross ⊗ indication.

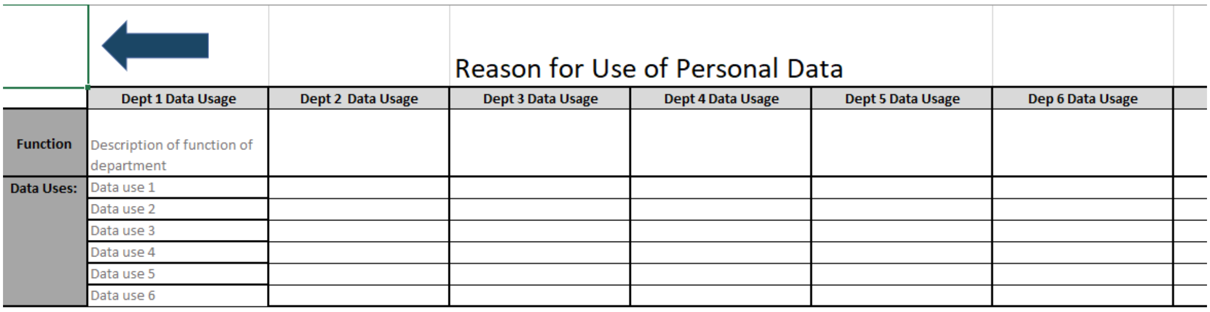
The red cross ⊗ indication will show that you have scored less than half of the possible 14 marks in that section.

Completing the ToolKit

Data Purposes

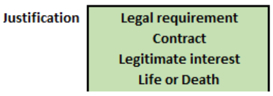
The first stage is to complete the 'Data Purposes' section of the tool kit

This allows you to identify, for each department in your organisation, the uses they have for personal data. The Toolkit allows for up to 9 departments, if you need more simply use a second toolkit.



Reason for Use of Personal Data

	Dept 1 Data Usage	Dept 2 Data Usage	Dept 3 Data Usage	Dept 4 Data Usage	Dept 5 Data Usage	Dep 6 Data Usage
Function	Description of function of department					
Data Uses:	Data use 1					
	Data use 2					
	Data use 3					
	Data use 4					
	Data use 5					
	Data use 6					



Justification	Legal requirement Contract Legitimate interest Life or Death

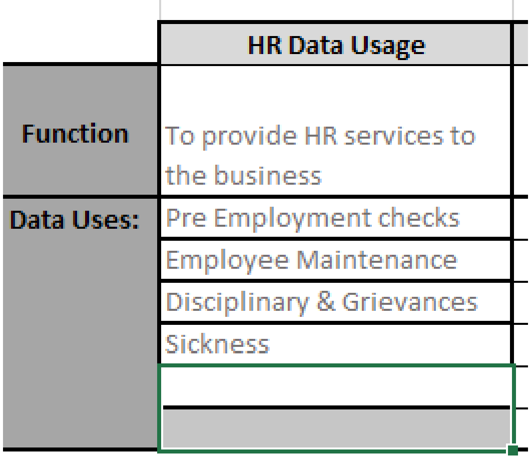
Use one column for each department to be assessed.

Change the Column heading to the department name, ‘Dept 1 Data Usage’ may become ‘HR Data Usage’ for example This name change is then reflected throughout the Toolkit.

Definitions
Data Purposes
HR Data Usage

Then enter a description of the function of that department.

Then enter the uses that that department has for personal data. These uses are used in the next steps when assessing the reasons for the data processing.

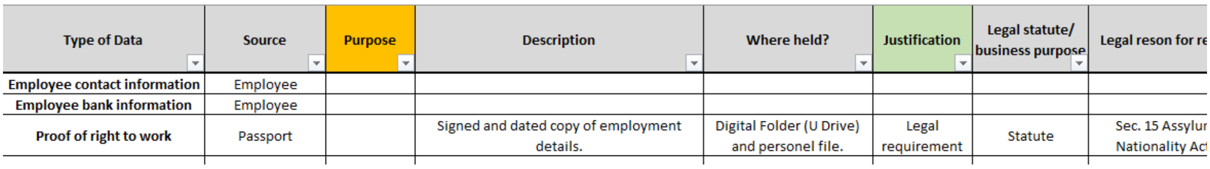


	HR Data Usage
Function	To provide HR services to the business
Data Uses:	Pre Employment checks
	Employee Maintenance
	Disciplinary & Grievances
	Sickness

Departmental Data Usage

Once the reasons for usage of personal data in each department has been identified and entered onto the ‘Data Purposes’ sheet you should then, for each department, identify the type of data being processed, its source, purpose and so on completing one row in the departmental sheet for each data usage identified in step one.

You should select the corresponding data usage from the drop-down selection list for each ‘row’. Where the processing of personal data has more than one ‘justification’, such as employee data needed for “legal requirements” such as entitlement to work checks, as well as payroll processing the more than one row may be needed.

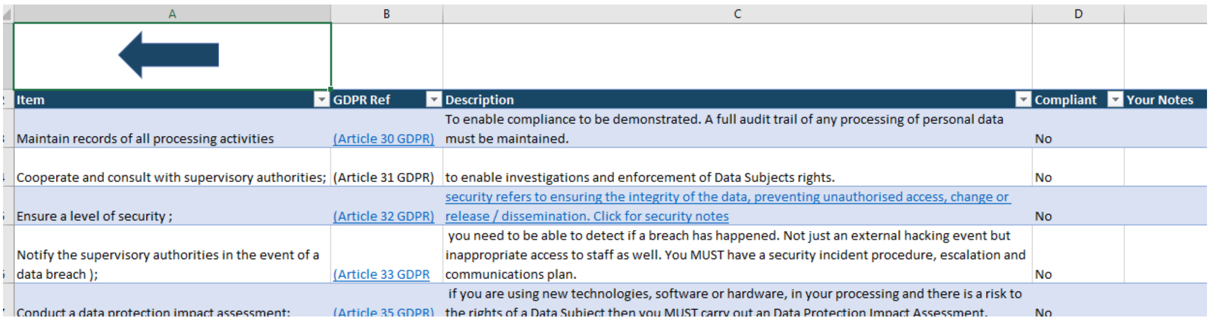


Type of Data	Source	Purpose	Description	Where held?	Justification	Legal statute/ business purpose	Legal reson for re
Employee contact information	Employee						
Employee bank information	Employee						
Proof of right to work	Passport		Signed and dated copy of employment details.	Digital Folder (U Drive) and personel file.	Legal requirement	Statute	Sec. 15 Assylur Nationality Act

Completing the compliance check list

Once all personal data processing in each department has been identified and recorded onto the departmental data usage sheets you can proceed to the assessment sheets.

Each area of the GDPR, Data Controllers responsibilities, Data Processors responsibilities and Data Subjects rights has a separate sheet where the major requirements of the GDPR in that area are listed.



Item	GDPR Ref	Description	Compliant	Your Notes
Maintain records of all processing activities	(Article 30 GDPR)	To enable compliance to be demonstrated. A full audit trail of any processing of personal data must be maintained.	No	
Cooperate and consult with supervisory authorities;	(Article 31 GDPR)	to enable investigations and enforcement of Data Subjects rights.	No	
Ensure a level of security ;	(Article 32 GDPR)	security refers to ensuring the integrity of the data, preventing unauthorised access, change or release / dissemination. Click for security notes	No	
Notify the supervisory authorities in the event of a data breach);	(Article 33 GDPR	you need to be able to detect if a breach has happened. Not just an external hacking event but inappropriate access to staff as well. You MUST have a security incident procedure, escalation and communications plan.	No	
Conduct a data protection impact assessment;	(Article 35 GDPR)	if you are using new technologies, software or hardware, in your processing and there is a risk to the rights of a Data Subject then you MUST carry out an Data Protection Impact Assessment.	No	

Based on your identification of the personal data processing being undertaken in each department you should select your compliance level against each of the criteria,

If for example you feel that the details all processing of personal data identified is fully recorded in a secure way then you could select ‘Yes’ for the first item in the ‘Data Controllers’ Sheet. If however you have identified that these is an area where records of processing is not as secure as you feel is needed then you should select Partial. If however there are areas where details of processing are not fully recorded then you should select ‘no’ from the compliant drop-down.

Details of the requirements for each item in each of the there GDPR areas can be found by following the links to the DGPR reference which gives the wording of the GDPR article itself.

GDPR Compliance Score

Based on your entries into each of the criteria in each area, Data Controllers responsibilities, Data Processors responsibilities and Data Subjects rights a overall score for each area will be calculated and displayed on the Compliance scoring section of the ‘GDPR Overview’ sheet.