

## Case Study 1 – Data Protection

Deadline: 14<sup>th</sup> January 2022, 8pm.

Peer Marking Deadline 28<sup>th</sup> January 2022, 8pm.

Marks 30% of unit mark.

Submit: Via moodle.

### Task

ACME Review Inc have built a successful online business providing a car review website. It collects the reviews from users and uses these to create overall scores for cars. This American company has decided to expand to the United Kingdom. To do this, they will need to comply with GDPR UK.

Its main source of income is paid-for advertising that is displayed alongside the car review details. When a user signs up, it asks for explicit permission to use information provided by the user to generate ratings for cars and to share individual review comments with site visitors. In addition to allowing the website user to pick a 'screen name' it also requires their real name, age, sex, city of residence and email address. This information is currently used along with the car rating information to help target advertising to individual users. It never shares this information with the advertisers and provides the user the ability to opt-out of the use of the data to select the adverts shown.

The company plans to introduce two new features:

1. It will recommend cars it thinks a user will like based on their having a similar profile of existing car ratings to other site users.
2. It currently does not have any kind of avatar image that is displayed when comments are shown. It will allow users to upload a small image to be used for this purpose. If a user has not upload an image, it plans to assigned a system generated cartoon 'face'. The construction of the face will be based on the additional information that users have previously provided to the company. The company believes this will be more effective than using a single standard blank face cartoon. It will also allow users to modify this cartoon. For example, by changing hair style, eye colour, add glasses and similar features.

In this exercise you will assess the compliance of the company against the requirements of the GDPR UK(General Data Protection Regulations) as brought into law by the Data Protection Act 2018 by providing answers to a series of questions.

The lecturer will take on the role of the Chief Information Officer of the company and answer any reasonable questions seeking clarification about current or planned data use. A specific forum will be created for this purpose so that everyone is working with common answers.

It is acknowledged that you are not legal experts, however as computing professionals specialising in data handling, you are expected to demonstrate an understanding of the principles behind the rules and identify best practice.

You may assume that Acme has decided to keep its life simple by making the UK rating site and company completely separate from the US one and will not share data between them, keeping the data collected in the UK. It will use the codebase of the existing website to create the new one and will make changes as required.

### Questions

You should provide answers to the following questions.

- Q1. Excluding accountability, what are the data privacy principles of the GDPR? You should provide a brief one or two sentence explanation for each, in your own words, not just a heading. [7 marks]
- Q2. Identify a change to the way the current US website works that the company will need to make to be compatible with the GDPR when it launches the UK version, and why this is necessary. [3 marks]

Q3. Indicate two actions the company will need to take in relation to the implementation of the new features described above, because of the GDPR Accountability principle. [4 marks.]

Q4. Identify a GDPR related issue that the company may have with implementing the plan to provide individualised recommendations and suggest a way these could be addressed to allow this to proceed. [3 marks]

Q5. When a user decides to close their account on the website, the company is required to delete their data. In order to continue to provide the useful ratings and review comments to other users, the company would like to turn this data into anonymous data by disconnecting it from the personal details (name, city, etc.) held about the user. It plans to seek permission to do this. Is the deleting of the personal data sufficient to achieve this? Explain why it is/is not sufficient. [4 marks]

Q6. Other than a lack of consent, suggest a reason that allowing the system to generate the avatar image in the way described would not be compatible with the GDPR. [3 marks]

Q7. Indicate an alternative approach that could be employed to provide a unique system generated avatar image for each user that would be compatible with the GDPR and would not leak any of the user details. And explain why this would be compatible. [4 marks]

All answers are expected to contain properly referenced citations of appropriate sources. Each part of the answer as indicated in the assessment criteria should only require a one to three sentence answer (excluding q1a.) When referencing a website, you should provide a specific page not just the site homepage.

A further two marks are awarded for properly formatting the submitted document. Proper formatting means that headings have been provided that break the document into sections that assist in identifying where the answers to the seven questions can be located. And that the references used follow the Bath-Harvard referencing style (<https://library.bath.ac.uk/referencing/harvard-bath>).

## Assessment Criteria

Marks will be allocated within a question as indicated in this section.

For each question, a set of model answers will be provided during the peer marking period. When peer marking, it is not necessary to match this word for word. Matching the intent will be sufficient to gain the mark. The list of model answers will be reasonably exhaustive, but any other answer that meets the objective should also receive the mark.

Assessment Criteria		
Question	Criteria	Marks
Q1.a.	Has each principle been given, with sufficient description? One mark for each.	6
Q1.b.	Has an appropriate reference been provided for the principles?	1
Q2.a.	Has a required change been given?	1
Q2.b.	Has the reason for the change been given?	1
Q2.c.	Has a suitable reference been given for the required action?	1
Q3.a.	Have two actions the company will need to take been given? One mark for each.	2
Q3.b.	Have suitable references been given for each action? One mark each.	2
Q4.a.	Has a relevant GDPR related issue with the proposed plan been identified?	1
Q4.b.	Has a viable suggestion been provided for how this issue could be addressed?	1
Q4.c.	Has a suitable reference for the issue and its resolution been provided?	1
Q5.a.	See model answer for guidance of suitable explanations.	3
Q5.b.	Has a suitable reference that assists in understanding the explanation been given?	1
Q6.a.	Has a valid reason why the proposed plan may not be appropriate been provided?	2
Q6.b.	Has a referenced been provided that assists in the understanding of the reason?	1

Q7.a.	Has a viable alternative solution been provided?	1
Q7.b.	Has an explanation of why this is an appropriate solution been provided?	2
Q7.c	Has a reference been provided that assists in assessing the validity of the solution?	1
Formatting	Is the document properly formatted. (1 mark for structure, 1 for referencing style.)	2

## Submission

You should submit a single pdf to moodle containing your answers. With the answers to each question clearly labelled. Do not include your name or user details in the content of the pdf or in the file name you choose to upload. Do not zip or otherwise compress your upload.

## Peer Assessment

This unit will make use of peer assessment. This means that after the initial deadline for a piece of coursework you will be allocated the work of three other students to examine and assign a mark. This will allow you to see how others have tackled the same problem. The purpose of this is to expose you to issues you may not have identified for yourself and improve your understanding of the problem being tackled.

You will be provided details of how to download the three submissions. You are expected to examine these and compare them to the assessment specification given in this document. Each of the criteria is designed to be a simple pass/fail assessment where the submission either meets the requirement or it does not. Where any criteria are not met, you must indicate why you have reached this conclusion.

You will be given a link to an online form where you can submit an entry for each submission you examine. You must also submit an entry for your own work. You are strongly recommended to assess your own work after you have reviewed the work of the other students. You must submit all the forms by the peer assessment deadline.

There are no additional marks for completing the peer assessment. However, a penalty of up to 50% will be applied to your lab mark should you fail to complete the peer assessment satisfactorily.

A satisfactory assessment entry means you will have completed a form for each submission allocated to you and provided a valid justification for each of the criteria you have labelled as not met.

The work you submit should be anonymous and not include your name or userid. You should remove any reference to your username in any pathname in your code. Replace it with 'username'. You must not engage in discussion of your mark or the marks you will allocate to your peers with your peers. You should report any attempt by others to influence the marking process.

## Mark Calculation

Your mark will be calculated in the following way:

1. The two closest peer marks given will be used. If the three marks are equally spaced, the pair closest to your own estimate will be used.
2. If your own mark estimate lies above the peer marks you will receive the mean of the peer marks.
3. Otherwise, you will receive the mean of the two highest marks. (The two peer marks and you own estimate.)

Your mark will be returned to you once this processing has been done. You will also receive the details of the marks allocated by your peers. This will include their reasoning. This is a provisional mark. If you do not consider the mark to be fair, you can contact the lecturer and ask for it to be reviewed. Your work will be re-marked and where the lecturer determines a different mark, the peer marking will be checked and any unsatisfactory marking will have the penalty applied. Should your request for a review not be justified, a penalty may be applied to your mark as you will have further demonstrated that you have not properly understood the material or the feedback you have received.

After the review period the coursework mark will be finalised. To maximise your marks, you should attempt to be as accurate in the marking of both the peer work and your own.

### Extensions

If any student is granted an extension, they will still have to undertake peer marking of others work after their updated deadline, with appropriate extensions. Their own work may be peer marked or assessed by the lecturers/tutors depending on the availability of peer markers at that time.

### Plagiarism

Plagiarism is a serious offence - please check: <http://www.bath.ac.uk/library/help/infoguides/plagiarism.html> and <http://www.bath.ac.uk/students/support/academic/academic-integrity/>