ClearCourse Events & Leisure
Data Processing Impact Assessment ("DPIA")
for new data analytics product: "Claritee" by ClearCourse

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Claritee consolidates and anonymises selected data held on golf club clients across ClearCourse companies for statistical, management and business development purposes through benchmarking.

The broad categories of data are:

- Golf club members
- Membership types and subscriptions
- Secondary expenditure (e.g. Green fees, food and drink)
- Golf activity and course utilisation

A registered user of one (of our golf club customers) can access details on the above data for their own club. They can also see summary statistics for other categories of clubs (e.g. average green fee for clubs in Oxfordshire), but cannot see details for another individual club. Where there are limited number of clubs in any given area, this feature will be limited to a wider-region to ensure any "motivated intruder" would not be able to "drill down" and identify any individuals through using the filters provided by the product.

Note that all of the above data is already held internally, being sourced from ClearCourse Golf Club management systems. This data has been collected and processed in line with our privacy policy, which states: "*We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose*"

Additionally, individual users of the system provide their name and email address in order to generate a user account. For security, these accounts are protected by multi-factor authentication (passwords and authenticator tools).

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

How will you collect, use, store and delete data?

Customers submit their name and email address via an online form, which is then used to create a user account.

All other club data is imported from other internal systems. The data is collated and anonymised for each participating club on a monthly basis to build aggregated sums or averages for each club without identifying individuals that are members of the clubs in order to uphold the principle of privacy by design and default and to ensure a low impact on any individuals' rights and to mitigate any concerns that might arise for any individual.

For further information on how data shall be anonymised, please see details within the embedded document below:

Claritee
Anonymisation (202

What is the source of the data?

A customer account allows them to access a subset of the data which they already access via one of Clearcourse's Golf Club management systems. Additionally, the system shares industry benchmarks for groups of clubs but does not share individual data items from other clubs.

Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows.

Data will be shared with our customers who subscribe to the Claritee product, and whom we have contractual terms in place which cover data processing activities.

What types of processing identified as likely high risk are involved?

Please see Step 5 and Step 6 of this DPIA below, we do not envisage any of the processing activities associated with this product as being categorised as "high risk".

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data, and does it include special category or criminal offence data?

Internal data on existing golf club clients. No special category or criminal offence data shall be processed as part of the Claritee product.

The only data items relating to individuals (golf club members) are:

      i.   Date of birth

     ii.   Gender

    iii.   Longitude and latitude coordinates of home address.

    iv.   Annual spend at the golf club

     v.   Date of joining the golf club

    vi.   Golf club membership category

Of the above data, only latitude and longitude are displayed in the product. The other items are used to calculate club-wide statistics (e.g. average age of members) but are not displayed individually.

Other than an internal ID number, there are no other personal details linked to these coordinates which would identify the individuals.

Categories of personal data processed as part of the Claritee product:

1. Names and email addresses submitted via the contact form, by those wishing to enquire about the product

2. Names and email addresses of registered users who have purchased the product

How much data will you be collecting and using?

The data types as set-out above shall be collected and used as part of this product. This is the minimum amount of data required to ensure effective use of the Claritee product for ClearCourse and its customers.

How often?

• Individuals that use Claritee (our customers' employees or approved users): their user ID and e-mail address will be processed as part of the log-in process.

• Individuals whose personal data has been anonymised: The data is anonymised as is it added to the Claritee product. From there the anonymised and aggregated data can be used by Claritee customers each time they log-in to use the product.

How long will you keep it?

The data will be "kept", stored and processed in line with our data retention and deletion policy.

How many individuals are affected?

This shall vary depending on the number of our customers which subscribe to the Claritee product.

What geographical area does it cover?

The Claritee is currently intended to cover the UK and Ireland. If this changes in the future this will be assessed and appropriate measures will be taken to ensure adequate safeguards are put in place.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals?

- Individuals that use Claritee: are our customer's employees or approved users.
- Individuals whose personal data has been anonymised: are our customers' customers.

How much control will they have?

The Claritee product provides a system that is read-only in operation and does not allow the data to be changed or removed.

Would they expect you to use their data in this way?

Yes. This processing activity is provided for in our privacy policies.

Do they include children or other vulnerable groups?

During the consultation call with external and internal legal counsel, a concern was identified in relation to processing of "junior membership" data which would involve the anonymisation of data relating to children. However, as it would be unlikely to return data for a single junior member (under the age of 18) for any given club, and also given that any such data would not be viewable by anyone other than an authenticated user, the data for other clubs/areas in the Claritee product will at most be aggregated sums or averages of spending behaviour of junior members, which would not affect or identify any individual.

Are there prior concerns over this type of processing or security flaws?

There are no prior or public concerns over this type of processing.

Is it novel in any way?

The Claritee product provides standard business analytics and benchmarking tools. This may be a new product for the golf sector but the processing itself is not novel.

What is the current state of technology in this area?

ClearCourse Events & Leisure are a market leader in the provision of business solutions for golf clubs in the UK. As such this business tool can be seen as a new technology offering in this specific area.

Are there any current issues of public concern that you should factor in?

There are no prior or public concerns over this type of processing.

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

What do you want to achieve?

The benefits of this data processing is to provide a benchmarking tool for customers to compare business data against similar organisations in the sector, both locally and nationally.

What is the intended effect on individuals?

This new processing activity is expected to have a medium to high benefit to the individuals whose data is processed in connection with the business activity. By using our data analytical and benchmarking tool, our customers (golf course and golf clubs) will be able to offer individuals more suitable and cost efficient products and offerings, however ultimately, this will be at the discretion of our customers.

What are the benefits of the processing – for you, and more broadly?

This new business activity offers huge potential benefit to ClearCourse Event & Leisure ("CCE&L"). This new business activity offers customers of CCE&L a new dynamic data analytics and benchmarking tool which shall allow them to compare business data against similar organisations in the sector, both locally and nationally.
This offering will allow CCE&L to increase revenues and to ensure we continue to offer market-leading sector-specific software products and services to our customers.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Consultation has taken place with a subset of consumers/data controllers, along with business consultants in the sector. Security consultation with project CTO and wider organisation technology leads has also taken place.

In May 2024, an in-depth product demonstration was carried out with members of the ClearCourse Legal Team as well as external legal consultants. Following this review, several recommendations were made to the product team in relation to processing activities with this product. It was also agreed that information will need to be supplied to our processors / joint data controllers as part of the roll-out of this product.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

what is your lawful basis for processing?

Legitimate Interests. Please see Legitimate Interest assessment report within the embedded document below "PID00100121_detailed_assessment_report_20240529":

PID00100121_detaile
d_assessment_report_

Does the processing actually achieve your purpose?

Yes.

Is there another way to achieve the same outcome?

Not currently.

How will you prevent function creep?

To ensure there is no function creep we only use data for the limited purposes explained in this DPIA. Any changes to the processing activities associated with this product will be brought to the attention of ClearCourse Legal and/or the ClearCourse DPO, who will decide whether to update this DPIA.

How will you ensure data quality and data minimisation?

The data processing activity for which ClearCourse shall be a data controller is the process of anonymizing golf club members data. The anonymisation process ensures data minimisation, while data quality and accuracy are maintained.

What information will you give individuals?

Individuals will have access to our privacy notices to ensure compliance with data protection transparency principles. Our privacy notices set-out how we shall process personal data, on what bases, and for what purposes. Individuals will be able to review our privacy policies and be able to contact us if they require any further information.

How will you help to support their rights?

We will be able to support individuals rights in the same way as usual, through the contact information provided on our privacy policies, we will be able to respond to any queries they may have. Our privacy notices set-out how we shall process personal data, on what bases, and for what purposes.

Additionally, a process has been adopted in order to limit any potential infringement of an individual's rights by broadly actioning and upholding any requests or complaints received by any individuals to remove their data from the Claritee system following any such request or complaint.

What measures do you take to ensure processors comply?

We intend to provide data processors and/or joint data controllers with hyperlinks to our privacy notice to ensure compliance with data protection transparency principles. Our privacy notices set-out how we shall process personal data, on what bases, and for what purposes. Individuals will be able to review our privacy policies and be able to contact us if they require any further information.

How do you safeguard any international transfers?

We do not envisage any international data transfers to third countries (without EU adequacy decisions, or UK adequacy regulation) to take place with this product. If this changes in the future this will be assessed and appropriate measures will be taken to ensure adequate safeguards are put in place.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
1. Unauthorised access to user accounts	Possible	Minimal	Medium
2. "Motivated Intruder" identifies an individual from the anonymised data set	Possible (but not likely)	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
1. Unauthorised access	Secure cloud-based system Multi-factor authentication	Reduced	Low	Yes
2. "Motivated Intruder" identifies an individual from the anonymised data set	Limit the ability for customers to apply filters where doing so could reduce the volume of the data set in such a way that an individual could be identified.	Accepted	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Vanessa Machin 09/07/2024	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Vanessa Machin 09/07/2024	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Simon Gyan – Group DPO, 05/07/2024	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:

The implementation of a secure cloud-based system and MFA are robust measures that significantly reduce the risk of unauthorised access. These measures are considered adequate for protecting information against unauthorised access. No further measures are required at this time as the risk has been effectively reduced to a low level.

Limiting the ability to apply filters that could lead to re-identification is a prudent step. This measure adequately manages the risk of identification by motivated intruders and is deemed sufficient.

Continue monitoring for any new techniques or potential vulnerabilities that could arise and adapt measures as necessary. Currently, no additional measures are required as the risk is managed to a low level.

Ensure that the measures to provide links to joint controllers as described in section 4 takes place.

The current measures for mitigating the risks of unauthorised access and the potential re-identification from anonymised data are adequate and effectively reduce these risks to a low level. Continuous monitoring and periodic reviews should be conducted to ensure these measures remain effective. **No additional measures are required at this time and processing may proceed.**

DPO advice accepted or overruled by:	Vanessa Machin	If overruled, you must explain your reasons
Comments: Accepted		
Consultation responses reviewed by:	Vanessa Machin	If your decision departs from individuals' views, you must explain your reasons
Comments: No deviation.		
This DPIA will kept under review by:	Vanessa Machin	The DPO should also review ongoing compliance with DPIA