London Youth Games
Data Protection Policy

Data Protection Policy

1. **Introduction**

London Youth Games (LYG) is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act"). This is the UK's implementation of the General Data Protection Regulation (GDPR), which came into force on 1 March 2000. The organisation will therefore follow procedures that aim to ensure that all employees, interns, volunteers, trustees, contractors, agents, consultants, professional partners, or other servants who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act. References in this Policy to "us", "we", "ourselves" and "our" are to London Youth Games. References to "you", "yourself" and "your" are to each worker to whom this Policy applies.

2. **Statement of policy**

To operate efficiently, LYG must collect and use information about people with whom it works. These may include members of the public, current, past, and prospective employees, volunteers, interns, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of regulators and other statutory bodies. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

LYG regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between LYG and those with whom it carries out business. LYG will ensure that it treats personal information lawfully and correctly.

To this end LYG fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

3. **The principles of data protection**

All our Workers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

We are not required to appoint a Data Protection officer. CEO is responsible for overseeing our compliance with data protection.

The Data Protection Act 2018 ("DPA 2018") applies to any personal data that we process. The data protection laws all require that the personal data be processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

The main themes of the data protection laws are:

- good practices for handling personal data
- rights for individuals in respect of personal data that data controllers hold on them; and
- being able to demonstrate compliance with data protection laws.

In summary, the data protection laws require us to:

- only process personal data for certain purposes
- process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure, processing it fairly and in a transparent manner and keeping it for no longer than is required)
- provide certain information to those individuals about whom we process
- personal data, which is usually provided in a privacy notice, for example we will have received one of these from us as one of our staff
- respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and

- keep adequate records of how data is processed and, where necessary, notify the regulator and possibly data subjects where there has been a data breach.

At the end of this document is an advice note on how to deal with a data breach.

Data protection law in the UK is enforced by the Information Commissioner's Office ("ICO") and they are the regulator for data protection in the UK. The ICO currently has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met
- collected for specific, explicit, and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation")
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation")
- accurate and where necessary kept up to date
- kept for no longer than is necessary for the purpose ("storage limitation")
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

These Principles are legally enforceable.

4. Data Protection Rights

Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

- The rights to access their personal data, usually referred to as a subject access request

- The right to have their personal data rectified
- The right to have their personal data erased, usually referred to as the right to be forgotten
- The right to restrict processing of their personal data
- The right to object to receiving direct marketing materials
- The right to portability of their personal data
- The right to object to processing of their personal data; and
- The right to not be subject to a decision made solely by automated data processing.

Not all these rights are absolute rights, some are qualified and some only apply in specific circumstances. More details on these rights can be found in Part 2 of this Policy.

The exercise of these Rights may be made in writing, including email, and verbally and should be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, considering the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

5. Our obligations

What this all means for LYG can be summarised as follows:

- We will treat all personal data with respect.
- Staff/Trustees/Volunteers will immediately notify their line manager or our CEOX, if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them
- We will take care with all personal data and items containing personal data we handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

- Immediately notify CEO if anyone becomes aware of or suspect the loss of any personal data or any item containing personal data.

6. Lawful processing of data

For personal data to be processed lawfully, we must be process it on one of the legal grounds set out in the data protection laws.

For the processing of ordinary personal data in our organisation these may include, among other things:

- the data subject has given their consent to the processing
- the processing is necessary for the performance of a contract with the data subject
- the processing is necessary for the compliance with at legal obligation to which the data controller is subject; or
- the processing is necessary for legitimate interest reasons of the data controller or a third party i.e. we are processing someone's personal data in ways they would reasonably expect it to be processed and which have a minimal privacy impact on the data subject or where there is a compelling justification for the processing.

7. Data categories

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and 'sensitive' personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data.
- That data and other information, which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of

opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinion.
- Religious or other beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Sexual orientation.
- Criminal proceedings or convictions.

8. **Handling of personal/sensitive information**

To lawfully process special categories of personal data we must ensure that one of the following conditions has been met:

- the individual has given their explicit consent to the processing
- the processing is necessary for the performance of our obligations under employment law
- the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or another extreme situation
- the processing relates to information manifestly made public by the data subject
- the processing is necessary for the purpose of establishing exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

- ensure that either the individual has given their explicit consent to the processing; or
- ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context.

9. Foreign transfers of personal data

Personal data must not be transferred outside the European Economic Area (EEA) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections.

These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or since the recipients own country's laws provide sufficient protection.

These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of our group of companies.

LYG must not under any circumstances transfer any personal data outside of the EEA without the line manager's or our CEO prior written consent. Approval must be sought prior to any transfer of personal data outside the EEA.

We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data outside of the EEA.

10. Notification and response procedure

If anybody receives a verbal request in relation to a Right, the following actions must be taken:

- pass the call or person to a supervisor/manager if. The supervisor/manager should make a written record of all relevant details and explain the procedure.

If possible, try to get the request confirmed in writing addressed to our CEO. If it is not possible to transfer the individual over then make a written record of the request and contact details for individual making the request; and

- inform our CEO of the request and pass them any written records relating to the request.

If a letter exercising a Right is received, then we will:

- pass the letter to the relevant supervisor/manager; the supervisor/manager must log the receipt of the letter with our CEO and send a copy of it to them; and our CEO will then respond to the individual on our behalf.

If an email exercising a Right is received by anyone, they we will:

- pass the email to their supervisor/manager; the supervisor/manager must log the receipt of the email with our CEO and send a copy of it to them; and CEO will then respond to the individual on our behalf.

Our CEO will co-ordinate our response which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request and the Right. Our CEO will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from our CEO should suffice in most cases.

Our CEO will inform the relevant management line of any action that must be taken to legally comply with any exercise of rights. Our CEO will also co-ordinate any additional activity required by our IT department to meet the exercise of any of the Rights.

The manager/senior manager who receives the request will be responsible for ensuring that the relevant response is made within the time required.

Our CEO reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by external legal advisors.

10. How to locate information for data subject right requests and requests for the right to be forgotten and response procedure

If we are responsible for carrying out or co-ordinating any searches for personal data, then this section will show our approach to carrying out the searches.

10.1 The personal data we need to provide in response to a subject access request, right to be forgotten or any other exercise of data subject rights may

be in several filing and/or network systems, so it is important to identify at the outset the type of information requested to enable a focused search.

10.2 However, we should note that the individual is not obliged to clarify the scope of what we will need to search for, so whilst we can ask, we may not receive a useful clarification or any response at all. In this case we still must comply with the original request.

10.3 Depending on the type of information requested, we may need to search all or some of the following:

- electronic systems (e.g. databases, networked and non-networked computers, servers, customer records, human resources records system, email data, CCTV).
- manual/paper filing systems (but only if they are 'structured filing systems', on which see below); and
- any data systems held externally by our data processors.

10.4 The relevant person must be notified with access and authorisations to the relevant system or files that need to be searched,

10.5 We are obliged to conduct a reasonable search of the relevant systems using the individual's name, employee or membership number, address, national insurance number, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different. The CEO services will assist with the scope of the search.

10.6 If information is not part of a structured filing system, it does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

10.7 To be a structured filing system, the system must be:

- contain information relating in some way to individuals. Usually, there would be more than one file in the system, or a group of information referenced by a common theme (e.g. an absence spread sheet). The files need not be in the same geographical location but could be dispersed over different locations.

- structured by reference to individuals (e.g. by name or employee or account number) or by reference to information relating to individuals (e.g. type of job or location, address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held; and
- structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced to easily indicate whether and where in the file data about the individual is located.

10.8 Therefore, a structured filing system which is subject to the data protection laws must have an external and internal structure which allows personal data about an individual to be located relatively easily without having to conduct a manual search of the entire file. If we must thumb through the whole file to find specific information, the file is not a structured filing system.

10.9 It might help to apply the 'temp test' to determine if a system is a relevant filing system. If a temp with no specialist knowledge of our internal processes and procedures could, if asked to retrieve information about a specified individual, identify that the system might hold such information and where in that system the information would be. If so, it will be a structured filling system.

10.10 The CEO should be liaised with in relation to the searches carried out and they will also liaise with our IT department in relation to searches of our IT systems.

11. Right of Access

This section contains the specific procedure to be followed where an individual exercises their right of access (also known as a data subject access request). The request need not refer to the Right, for instance, it might simply request 'a copy of all the information that you have about me'.

11.1 There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

11.2 The data protection laws give individuals the right to obtain:

- confirmation that their personal data is being processed.
- access to their personal data; and
- access to other supplementary information.

11.3 The individual is entitled to receive a description of the following:

- the purposes for which we process the data.
- the categories of personal data we process about them.
- the recipients to whom we may disclose the data.
- the duration for which the personal data may be stored.
- the rights of the data subject under the data protection laws.
- any information available regarding the source of the data where it is not collected from the data subject direct.
- the right of the data subject to make a complaint to the supervisory authority for data protection.
- the logic behind any automated decision we have taken about him or her (see below), the significance and consequences of this automated processing.

11.4 Plus we must also provide the information constituting the individual's personal data which is within the scope of their request. We must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically, we can, unless the data subject specifies otherwise, also provide the information in electronic form.

11.5 If the individual requests details on automatic decisions made about him, we must provide appropriate information, but in a format that does not compromise any trade secrets.

11.6 We may:

- ask for additional information to confirm the identity of the individual making the request.

- request that the scope of the request is narrowed to ease the searches to be undertaken (but the individual does not have to agree to such a request from us); and
- where requests are manifestly unfounded or excessive because they are repetitive: (a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or (b) or refuse to respond. Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

11.7 Where we process a large quantity of information about an individual, the data protection laws permit us to ask the individual to specify the information the request relates to. The legislation does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

11.8 We should verify the identity of the person making the request, using "reasonable means" if we are not sure about their identity.

12. Redactions

12.1 Where we are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. They are not entitled to see information which relates to other individuals or to other people, e.g. to a company.

12.2 In these cases we would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

13. Disclosing personal data relating to other individuals

13.1 Sometimes information that is determined to be personal data about one I individual might include information identifying or personal data about another person (e.g. an email between two people might contain personal information relating to both the sender and the recipient) and in some cases it is not possible to redact the information about the other person. There are additional steps to consider in relation to whether we disclose this information.

13.2 We must consider whether the other person has consented to the disclosure of their information or whether it would be reasonable to comply with the request without the other person's consent.

13.3 Where the other person has consented, their information can be disclosed.

13.4 Where the other person has not consented, whether it would be reasonable to disclose that person's information will depend upon all the circumstances and we must assess these on a case-by-case basis.

13.5 We would consider whether:

- The other person has refused their consent.
- The other person's consent cannot be obtained (e.g. because they are incapable of giving it due to illness or incapacity).
- Asking for consent might reveal the identity of the individual making the request.
- We owe the other person a duty of confidentiality.
- We have taken any steps to obtain the consent of the other person.
- The other person is a recipient or one of a class of recipients who might act on the data to the individual's disadvantage.
- The other person is the source of the information.
- The information is generally known by the individual; and
- The individual has a legitimate interest in the disclosure of the other person's information which they have made known to us.

13.6 If we decide that the other person's information should be withheld (usually it should be), we still must provide as much of the information requested as we can. Therefore, we should protect the other person's identity by redacting as much of this information and other identifiable particulars.

13.7 We will always keep a record of what we have decided to do and our reasons for doing it.

14. Exemptions to the right of subject access

In certain circumstances we might be exempt from providing personal data in response to a subject access request. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

14.1 Crime detection and prevention

- We do not have to disclose personal data that we process for the purposes of preventing or detecting crime, apprehending, or prosecuting offenders, or assessing or collecting any tax or duty, if and to the extent that giving subject access would be likely to prejudice any of these purposes.

14.2 Confidential references

- We do not have to disclose certain confidential references that we have given to third parties but might have to disclose confidential references that we receive from third parties. Bear in mind that references received from third parties may contain personal data of another person, we must consider the rules regarding disclosure of other party's personal data set out above.

14.3 Legal professional privilege

We do not have to disclose any personal data that is legally privileged. The following would be legally privileged:

- confidential communications between us and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice; and
- confidential communications between us or our lawyers and a third party (e.g. a witness) where the dominant purpose of the communication is to give or seek legal advice in respect of current or potential legal proceedings. This claim to legal privilege would end as soon as the case has been decided and, at that moment, the documents in the file might be disclosable if a subject access request is received.

14.4 Management forecasting

- We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any organisation or any other activity (e.g. staff relocations, redundancies, succession planning, promotions, and demotions) if and to the extent that disclosing the personal data would be likely to prejudice the conduct of that organisation or activity.

14.5 Negotiations

- We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual were doing so would be likely to prejudice those negotiations.

In any cases of doubt then speak to the CEO and it may be that external legal advice is necessary in relation to whether an exemption can be applied in a particular case.

15. Right to Erasure

15.1 The right to erasure is also known as 'The right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

15.2 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

- where their personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- when the individual withdraws consent (but only to the extent that consent is the only basis for processing their personal data).
- when the individual objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing.
- where their personal data was unlawfully processed.
- where their personal data must be erased to comply with a legal obligation; and

- where their personal data is processed in relation to the offer of information society services to a child.

15.3 There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request:

- to exercise the right of freedom of expression and information.
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest.
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

15.4 If we have disclosed the personal data to be erased to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

16. Right to rectification

16.1 An individual has the right to ask us to:

- correct inaccurate personal data.
- complete information if it is incomplete; and
- delete personal data which is irrelevant or no longer required for our purposes.

16.2 If we have disclosed the personal data in question to third parties, we must inform them of the rectification request where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

16.3 If data is factually correct and we are justified in keeping it, i.e. it is relevant to the lawful purpose we are holding it for then we do not have to change or delete it, but the individual may make a request for erasure, i.e. the right to be forgotten, and in that case, we would have to analyse the personal data and whether we can retain it based on that Right.

16.4 Where we are not taking any action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority (usually the ICO) and to seek a remedy from the Courts.

17. Right to Restrict Processing

17.1 An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

17.2 We will be required to restrict the processing of personal data in the following circumstances:

- where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data.
- where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual.
- when processing is unlawful, and the individual opposes erasure and requests restriction instead; and
- if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

17.3 Previously given consent for processing can be revoked at any time by the individual, therefore we cannot justify continued processing of data because of a previous consent.

17.4 The individual does not have this right if the individual has entered a contract with us and the processing is necessary for the fulfilment of that contract.

17.5 We must inform individuals when we decide to lift a restriction on processing (for example, if an individual contested our right to process their personal

data on legitimate interest grounds and we subsequently found that our processing was justified on these grounds).

17.6 If we have disclosed the restricted personal data to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

18. The Right to Data Portability

18.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

18.2 The right to data portability only applies:

- to personal data an individual has provided to a data controller.
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

18.3 We must provide the personal data in a structured, commonly used, and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

18.4 If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

18.5 It is not expected that this right will impact upon as we do not process personal data by automated means.

19. Right to Object

19.1 Individuals have the right to object to:

- processing based on legitimate interests.

- the performance of a task in the public interest/exercise of official authority (including profiling).
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

19.2 If we process personal data based on our legitimate interests or the performance of a task in the public interest/exercise of official authority:

- individuals must have an objection on "grounds relating to his or her particular situation"; and
- we must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or the processing is for the establishment, exercise, or defence of legal claims.

19.3 If we process personal data for direct marketing purposes:

- we must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.
- we must deal with an objection to processing for direct marketing at any time and free of charge; and
- we must nevertheless comply with the terms of the Privacy and Electronic Communication Regulations and the e-Privacy Regulation which replaces it.

19.4 If we process personal data for research purposes:

- individuals must have "grounds relating to his or her particular situation" to exercise their right to object to processing for research purposes; and
- If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

19.5 If our processing activities fall into any of the above categories and are carried out online, we must offer a way for individuals to object online.

19.6 We must inform individuals of their right to object "at the point of first communication" and in our privacy notices. This right must be "explicitly brought to the attention of the data subject and is to be presented clearly and separately from any other information".

20. Automated decision making and profiling

20.1 The privacy legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

20.2 We do not currently undertake any automated decision making. We must identify any of our subsequent processing operations that constitute automated decision making.

20.3 Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

20.4 We must ensure that individuals are able to:

- obtain human intervention.
- express their point of view; and
- obtain an explanation of the decision and challenge it.

20.5 The right to obtain human intervention does not apply if the automated decision is:

- necessary for entering into or performance of a contract between us and the individual.
- authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- based on explicit consent (but bear in mind that any consent can be withdrawn).

20.6 The data protection laws define profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, to analyse or predict their:

- performance at work.

- economic situation.
- health.
- personal preferences.
- reliability.
- behaviour.
- location; or
- movements.

20.7 When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place. We must:

- ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- use appropriate mathematical or statistical procedures for the profiling.
- implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

20.8 Automated decisions taken for the purposes must not concern a child. Automated decisions must not involve or be based on the processing of special categories of data or criminal history records (previously sensitive personal data) unless:

- we have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest based on EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual; and
- (in each case) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

21. Enforcement

21.1 If an individual disagrees that we have properly complied with a Right or we fail to respond they may apply to a Court for an order or complain to the ICO in each case requiring us to properly perform the Right.

21.2 If the Court or the ICO agrees with the individual it can:

- order us to properly carry out the Right and what steps are needed to do this; and
- order us to notify third parties who we have passed the data onto of the Right.

21.3 A court can also award compensation to the individual for any damage they have suffered because of our non-compliance. The ICO can also impose a civil fine upon us. These fines can be very substantial

22. Deleting personal data in the normal course

22.1 We are only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, we can carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

22.2 What we cannot do is amend or delete data because we do not want to supply it or because of the exercise of a Right.

Summary

All trustees, members and authorised officers are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within LYG will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure and will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected using secure passwords, which where possible have forced changes periodically.
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of LYG must:

- Ensure that they and all their staff who have access to personal data held or processed for or on behalf of LYG, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between LYG and that individual, company, partner, or firm.
- Allow data protection audits by LYG of data held on its behalf (if requested).
- Indemnify LYG against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by LYG will be required to confirm that they will abide by the requirements of the Act about information supplied by LYG and will be provided access to our Privacy policy.

Implementation

The accountable officer within LYG for Data Protection is the Chief Executive, with day to day responsibility for implementation and management to the CEO. These officers will be responsible for ensuring that the Policy is implemented and maintained. The CEO will also have overall responsibility for:

- The provision of cascade data protection training, for LYG staff.
- For the development of best practice guidelines.
- For carrying out appropriate compliance checks to ensure adherence, with the Data Protection Act.

Definitions under DPA 2018

- **Personal data** is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, member, coach, athlete, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

- Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do if taken together with other information available to or obtainable by us (e.g. a job title and company name). More details on this can be found in part 2 of this Policy.
- **Data subject** is the living individual to whom the relevant personal data relates.
- **Processing** is widely defined under the data protection laws and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure, or destruction of personal data, including CCTV images.
- **Data controller** is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.
- **Data processor** is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

Examples of information **likely** to constitute personal data:

- Names together with email addresses or other contact details.
- Job title and employer (if there is only one person in the position).
- Video - and photographic images.
- Information about individuals obtained because of Safeguarding checks.
- Medical and disability information.
- Member profile information (e.g. marketing preferences); and
- Financial information and accounts (e.g. information about expenses and benefits entitlements, income, and expenditure).

Examples of information **unlikely** to constitute personal data:

- Reference to the individual's name in a document that contains no other personal data about that them (e.g. including the individual in a list of

attendees of a meeting where the individual attended in an official capacity on behalf of a company); and

- Where the individual's name appears in an email that has been sent to or copied to them, but where the content is not about him or her (e.g. emails sent to the individual about an organisation's dealings).

Advice Note on Data breaches and self-reporting

This note focuses on the key legal elements of responding to a breach of personal data security, principally the obligation to notify data protection authorities or data subjects.

1. What is a breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can therefore include:

- access of a database by an unauthorised third party.
- sending personal data to the wrong recipient.
- devices such as USB sticks, laptops or mobiles containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability (even if it is just temporary) of personal data, for example, where there has been a back-up failure.

2. When do we have to report a breach?

All personal data breaches must be recorded if LYG is the data controller of the relevant personal data, including the facts relating to the personal data breach, the effects of the breach and any remedial action taken in response *(Article 33(5), GDPR)* as data protection authorities may demand the right to inspect these records. However, only certain personal data breaches must be proactively notified to the relevant supervisory body and individuals concerned.

As well as reporting the breach to the relevant body, LYG will also need to inform the insurer

2.1 Supervisory Authority

Notification to the ICO is only triggered where a breach is likely to result in a risk to individuals' rights and freedoms. *(NB: in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. Further guidance is available on the ICO website.)*

When assessing the risk to individuals, LYG will need to consider the specific circumstances of the breach, including the likelihood, severity, and potential impact of the risk. The Article 29 Working Party (**WP29**) (which was set up to provide the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States) recommends considering the following factors when assessing risk:

Type of breach.

Nature, sensitivity, and volume of personal data.

How easy it is to identify individuals.

How severe the consequences are for individuals?

Special characteristics of the individual (for example, children or other vulnerable individuals may be at greater risk).

Number of individuals affected.

Specific characteristics of the data controller (for example a sports organisation processing large amounts of special categories of personal data will pose a greater threat than the mailing list of a club).

Example

The ICO recommends that where there has been theft of a database e.g. for your membership contracts where you hold any payment or bank details for those members, the data of which may be used to commit identity fraud, your members would need to be notified, given the impact this is likely to have on those individuals who could suffer financial

loss or other consequences. On the other hand, it suggests that you would not normally need to notify the ICO, for example, about the loss or alteration of a staff telephone list.

2.2 Individuals

The requirement to communicate a breach to individuals is triggered where a breach is likely to result in a high risk to their rights and freedoms. The same factors listed above at paragraph 2.1 should be applied in assessing whether notification to individuals is required. WP29 suggests a presumption of high risk to individuals where the personal data involved is special categories of data. In practice, where notification to individuals is required, notification to the relevant supervisory authority will always be required.

Whether individuals should be notified will depend on the circumstances of the breach. For example, a loss of data which can be confirmed as encrypted and where the key has not been compromised, may represent a very low risk, and would not require notification to individuals (or indeed the supervisory authorities). However, even where data is encrypted, if there are no comprehensive backups of the data, then this could have negative consequences for individuals which could require notification.

NB: the ICO has the power to compel us to inform affected individuals if it considers there is a high risk.

Example

If LYG suffers a breach that results in an accidental disclosure of some of its "participants" medical records, there is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.

3. What information needs to be contained in the notification?

3.1 Supervisory authority

The following information needs to be provided:

3.1.1 A description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.

3.1.2 The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.

3.1.3 A description of the likely consequences of the personal data breach.

3.1.4 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

3.2 Individuals

The following information needs to be provided:

3.2.1 The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.

3.2.2 A description of the likely consequences of the personal data breach.

3.2.3 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

In practice, the ICO or other supervisory authority may assist a controller in identifying what information should be communicated to individuals. Dedicated messages to individuals about data breaches should not form part of any press release or other media statement unless there are no other means of contacting the individuals.

4. When does the data breach need to be notified?

4.1 Supervisory Authority

LYG as a data controller must notify a data breach to a supervisory authority promptly, and where feasible, not later than 72 hours after having become aware of the breach. A controller is deemed to become aware of a data breach when the controller has "*a reasonable degree of certainty*" that the incident affects personal data.

For example, the 72-hour countdown will start as soon as we realise an unencrypted CD or other removal storage device with personal data has been stolen. Even though you may not understand how the breach has taken place, we

will still have a *'reasonable degree of certainty'* that it has taken place. On the other hand, where you need to gather some evidence to establish *'with a reasonable degree of certainty*' that the suspected data breach has occurred, WP29 recognises that you may need

a "short period of time" to perform an investigation before the clock starts. Although there is not a set deadline for this preliminary investigation and assessment, actions to investigate should be carried out as soon as you find out about a suspected breach. If you fail to carry out any preliminary investigation (e.g. by ignoring an alert or suspicion that a breach may have occurred) or you do not carry out an investigation promptly, you may be held accountable for a breach of your obligations under Article 32 GDPR**.**

However, where you are in doubt, you should still make an interim notification in such circumstances until more is known. There will be no penalty for making a notification which ultimately turns out *not* to be a breach, but please be aware that notifying the ICO or such other regulator about a security incident does run the risk of investigation into the adequacy of security measures, even if it turns out that no harm has been done on that occasion.

4.2 Individuals

There is no set deadline for notifications to individuals, but this must be done without undue delay and will ultimately depend on the circumstances. For example, where financial information has been lost, the need to mitigate an immediate risk of damage would call for immediate communication to those individuals affected to give them the opportunity to change their passwords, security details etc.

ICO advises that normally data subjects will be notified after the supervisory authority, and following advice from such authority, but recognises that this will not always be the case, and importantly, that notifying the authority will not serve as a justification for failure to communicate to data subjects. In other words, do not wait for advice from ICO if the individuals affected are plainly at risk in the meantime.

5. What if we do not have all the information available yet?

If we do not have all the necessary information within 72 hours of when we become aware of the data breach, it is still possible to provide this information in phases, provided further information is provided to the ICO promptly. The presence of this option to notify in stages will make it difficult for any organisation to argue that it is not feasible to make any notification within 72 hours.

6. What if we fail to report a breach?

Failing to notify a breach when required to do so could result in administrative fines of up to EUR10 million or 2% of annual global turnover. However, if we fail to take appropriate security measures against data breaches in accordance our obligations under the Accountability principle (Article 5, GDPR) (***See Advice note on Accountability***) we may be

subject to fines up to the higher threshold of fines i.e. EUR20 million or 4% of the annual global turnover.

Date of review: 27 January 2021

Date of next review: