TALENT
WITHOUT
LIMITS

RECRUITMENT OF STAFF (INCLUDING CONSULTANTS PRIVACY NOTICE

JULY 2022

Version: 2.0

GLOBAL

GDPR compliant

WHY DO WE HAVE THIS PRIVACY NOTICE?

We are Gymshark and treating individuals and their personal information with respect reflects our core values and the values of our brand(s). So we want you to know as much as possible about what we do with your personal information. Also you and your personal information are protected by various laws and guidance and Gymshark is committed to upholding these and respecting your privacy and keeping your information safe. So whilst this privacy notice is quite long, we want you to be fully informed. We look forward to welcoming you to the Gymshark family. Please note while you read it, that not all parts of this privacy notice may apply to you depending upon the nature of your role with us that you are applying for.

In this privacy notice any reference to "us", "we", "our" or "ourselves" is a reference to Gymshark, and the particular part of the Gymshark group that you work for and any reference to "you", "your" and "yourself" is a reference to you as an applicant to become one of our staff or to start working for us.

This privacy notice applies to all past, current and future job applicants for positions to work for Gymshark, whether the position is based at one of our premises (including our retail stores, offices or any other physical premises owned or leased by Gymshark) or remotely. You may be applying to work for as an employee, director, temporary worker or consultant. This privacy notice provides details in accordance with applicable data protection laws about how we collect and use personal information about you during and after our recruitment process.

Please note that we have a separate privacy notice that relates to personal information captured by our CCTV and Access Control systems at our premises (including where you may be working or visiting our stores and/or workout spaces). A copy can be found at www.gymshark.com/pages/gymshark-privacy-notice. We have a separate privacy notice that applies to our customers and potential customers, a copy of which can be found at www.gymshark.com/pages/gymshark-privacy-notice so this will apply if you purchase products from us (whether in store or online), use our Gymshark app(s), add yourself to our marketing database, enter any of our promotions/competitions, apply to attend any of our events, visit our stores or workout spaces or you have an unpaid active social media relationship with us. Finally we have a separate Rest of the World privacy notice that applies to any other individual that may interact with us, a copy of which can be found at www.gymshark.com/pages/gymshark-privacy-notice and this covers everyone else including influencers or athletes who have a business relationship with us. This privacy notice does not apply to you therefore to the extent you are an athlete or influencer that we work with or applies to work with us. You should also read these privacy notices to the extent that they will apply to your activities/interaction with us in addition to this privacy notice.

We also have a separate privacy notice that will apply to you if you are successful in your application to work for us, and we will provide that to you once you are successful in your application as part of your joining process.

THE CONTROLLER OF YOUR PERSONAL INFORMATION

For the purposes of data protection laws and this privacy notice, the controller of your personal information is whichever part of the Gymshark group is processing your personal information. This will usually be the part of the Gymshark group that you are applying to work for. Being a controller of your personal information means that we are responsible for deciding how we hold and use your personal information. Our main trading entity is Gymshark Limited (Reg No 08130873) which is incorporated in England and Wales. If you are based in the UK then this company will be the controller of your personal information. If you are based outside of the UK then the controller of your personal information will be the part of our group that you apply to work for. Sometimes we may pass personal information to different parts of our group, so this privacy notice covers our whole group and more than one part of our group may be a controller of your personal information. However regardless of where you are based in the world , any queries you have regarding your personal information will be dealt with by Gymshark Limited, which can be contacted at dpo@gymshark.com.

YOUR DUTY TO INFORM US OF CHANGES

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the period of your application to work for us. We

may also hold your records on file for future positions even if you are unsuccessful in your initial application to join us, so again ideally please update us with any changes.

WHAT IF YOU DO NOT PROVIDE PERSONAL INFORMATION?

Failing to provide some of the personal information we require may mean that your application to join us will not be successful and we are unable to consider you for the position you are applying for.

Certain information (depending on the extent of your relationship with us), such as contact details, your right to work in the UK and payment details, must be provided to enable us to enter into a working relationship with you.

IF YOU HAVE QUERIES OR CONCERNS JUST ASK!

We have appointed a data protection officer (DPO) to oversee our compliance with applicable data protection laws. If you have any questions about this privacy notice or how we handle your personal information, please contact our DPO at dpo@gymshark.com.

CHANGES TO THIS NOTICE

We keep all of our privacy notices under regular review and we may update this privacy notice at any time. The current version of this notice is available via our Applicant Tracking System (ATS) or by requesting a copy from dpo@gymshark.com. If there are any material changes to this privacy notice in the future we will let you know, usually by updating the version on our website.

DATA PROTECTION PRINCIPLES

We are committed to being transparent about how we collect and use your personal information and in meeting our data protection obligations. Data protection laws say that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

To make sure this happens we are required under applicable data protection laws to notify you of the information contained in this privacy notice. It is important that you read this document before you make your application to join us so that you understand how and why we will process your personal information.

WHAT PERSONAL INFORMATION DO WE COLLECT?

In connection with your application to work with us, we may collect and process a wide range of personal information about you. This includes:

- Personal contact details such as name, title, address, email address and telephone number(s).
- Information about your date of birth, age, gender, marital status, referees, next of kin, beneficiaries, dependants, family members and emergency contacts.
- Bank account details, payroll records, national insurance number, tax records/status information and other tax or governmental identifiers.

- Information about your remuneration, including bonuses, entitlement to benefits such as pensions or insurance cover.
- The terms and conditions relating to you coming to work for us.
- Any communications between ourselves and you.
- Details of your previous schedule (days of work and working hours) and attendance at work.
- Details of previous periods of leave taken by you, including holiday, family leave and sabbaticals, and the reasons for the leave.
- Your usage of the IT systems we make available to visitors to our premises such as any visitor internet facilities at our premises.
- Identification information including your driving license and/or passport and background checks.
- Recruitment information including information about your nationality and entitlement to work in the UK, references, CVs, application information, past experience, reasons for leaving previous positions.
- Past work records including your qualifications, skills, experience, working hours, location of workplace, promotions, work titles, performance information, performance reviews, performance improvement plans, training records and professional memberships, attendance at events, start and end dates.
- Vehicle registration number, make and model if you are driving to visit us at our premises.
- Details of any past disciplinary or grievance or performance related procedures in which you have been involved, including any warnings issued to you and related communications.
- CCTV footage and other information obtained through electronic means such as swipe card records and access control systems if you visit our premises (see our separate CCTV and Access Control privacy notice at www.gymshark.com/pages/gymshark-privacy-notice).
- Photographs, video footage and audio recordings, for example any created as part of our assessment process.
- Results of HMRC employment status check, details of your interest in and connection with any intermediary through which your services are supplied.
- Information from Companies House.
- Shareholding, options, stock appreciation rights, dividend entitlements and investments you hold where relevant.
- Any other personal information you provide to us.

We may also collect and process more sensitive special category personal information including:

- Information about your health including any medical condition, health, and sickness records, including:
    - where you have a disability or medical condition for which we need to make reasonable adjustments.
    - where you stop working for a previous organisation and the reason for leaving is determined to be ill-health, injury, or disability including any records relating to that decision.
    - details of any past absences (other than holidays from work) including time on statutory parental leave and sick leave and the reasons for those absences.

- information about your health in the context of providing you with benefits as part of your proposed remuneration, for example health insurance.

- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or beliefs.

- In cases where it is relevant, we may also collect criminal records information about you, for example points on a driving licence where we need to ensure you are insured to drive any of our vehicles if this is relevant to the role you are being considered for, or an offence committed by you or alleged to have been committed by you impacts on your application to work for us.

If you are providing us with details of referees they have a right to know and to be aware of what personal information we hold about them, how we collect it and how we use and may share that information. Please share this privacy notice with them. They also have the same rights as set out in this privacy notice in relation to their personal information that we collect.

WHERE DO WE COLLECT YOUR PERSONAL INFORMATION FROM?

Gymshark collects your personal information in a variety of ways and from a variety of sources as set out below:

- Most of your personal information is collected directly from you, for example through application forms, CVs or resumes; from your passport or other identity documents such as your driving licence; from correspondence with you; or through interviews, meetings or other assessments, when you visit our premises or other personal information you provide to us.

- If you are applying for a position with us through a third party, then instead we may collect a lot of your personal information from the relevant recruitment agencies, temporary worker agencies, recruitment websites or platforms that have your personal information and which supply it to us or make it available to us.

- Third parties such as organisations you have worked for in the past or referees whose details you provide to us, Companies House, professional or trade organisations.

- From our information technology and communications systems, access control systems and CCTV and suppliers we use in connection with them.

- From the internet and social media and other public sources.

- From third parties appointed by you, for example any financial or legal advisors.

- From third parties appointed by us, for example a legal advisor appointed by us or a background check provider that we use.

- From government or government related bodies, regulators, the police, law enforcement authorities or the security services.

We store personal information relating to you in a range of different places, but mainly in our people management systems and in other information technology systems (including our email system, access control systems, in store monitoring and CCTV systems).

WHAT ARE OUR BASES FOR PROCESSING YOUR PERSONAL INFORMATION?

We will only use your personal information when the law allows us to. This means we must have one or more legal bases to use your personal information. Most of these will be self-explanatory. The most common legal bases which will apply to our use of your personal information are set out below:

- Where we need to perform the contract we have entered into with you which covers your working relationship with us or to take steps to enter into that contract.

- Where we need to comply with a legal obligation which applies to us, for example complying with health and safety laws.

- Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests. We have set out in the section below how we use your personal information together with more details on our legitimate interests.

- You have given your consent. Generally we do not rely on or need your consent for almost all uses we make of your personal information.

Where we are processing any sensitive special category personal information about you (for example personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, , data concerning health or data concerning a natural person's sex life or sexual orientation) we also need to have one or more of the following legal bases for using your personal information.

- Where we have your explicit consent to do so, for example to process your medical information to check we can provide you with health insurance as a benefit as part of your proposed remuneration.

- Where it is necessary for us to comply with our obligations and exercising our rights in the field of employment law, social security law and social protection law.

- Where we need to protect your vital interests (or someone else's vital interests).

- Where you have already made public the personal information.

- In establishing, exercising or defending legal claims, whether those claims are against us or by us.

- Where it is necessary in the public interest.

In cases where we do process special category personal information about you it will generally be to comply with legal obligations, where you have given your consent or to establish, exercise or defend legal claims.

In some cases more than one legal bases may apply to our use of your personal information.

HOW WILL WE USE YOUR PERSONAL INFORMATION?

There are many ways we will need to use your personal information during the application process with us. We have set out the main uses below, and indicated the main applicable legal bases of processing, but there may be other specific uses which are linked to or covered by the uses below.

- We will process your personal information to decide whether to enter into a working relationship with you. For example, we need to process your personal information to provide you with a contract and decide what terms will apply to any offer made to you. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests. We may also in some limited cases rely on your consent.

- We also need to manage our relationship with you, which may involve interviews, assessments, communications with you, decisions regarding your application. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests.

- As a business we have many legal obligations connected to your application to work for us or connected to visiting our premises which we need to comply with, for example, checking entitlement to work in the UK, to comply with health and safety laws, to make reasonable adjustments at any of our premises to accommodate a disability, to comply with data protection laws, to ensure equality and equal opportunities in our business or to invoke other legal rights.

- We will also need to keep and maintain proper records relating to your application to work with us and information about you which is relevant to the role you have applied for. As well as relating to

the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests, and we may also have legal obligations to do this.

- In some cases we may need to process your personal information to prevent, detect or prosecute criminal activity. This will also be in our legitimate interests, we may also have legal obligations or be exercising a legal right to do this and it will also be in the public interest.

- We may need to gather evidence for and be involved in possible legal cases. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests, we may also have legal obligations or be exercising a legal right to do this and it may also be needed to establish, bring or defend legal claims.

- To manage and keep a record of your application, any interviews or assessments and our decisions. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests, and we may also have legal obligations or be exercising a legal right to do this.

- Ensure effective general human resources and business administration and to manage our business. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests, and we may also have legal obligations or be exercising a legal right to do this.

- Obtain references from other organisations you have worked for or from referees whose details you provide. As well as relating to the entry into of a contract with you either directly or indirectly, this will also be in our legitimate interests, and we may also have legal obligations or be exercising a legal right to do this.

- Monitor any use you make of our information and communication systems to ensure compliance with our information technology policies, ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution and use of social media. This will also be in our legitimate interests, and we may also have legal obligations or be exercising a legal right to do this. In relation to social media you may also have already made the personal information public.

- We may need to process your personal information to help train our staff, and make sure they deliver the high standards expected in relation to our brand. This will be in our legitimate interests.

- Conduct data analytics studies to review and better understand staff recruitment and other trends in applications to join our workforce. This will also be in our legitimate interests, and we may also have legal obligations or be exercising a legal right to do this. We may anonymise and aggregate personal information for insight and research purposes, but this information will not identify you.

CHANGE OF PURPOSE

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. Our main purpose is to collect personal information about you to decide whether to recruit you now or in the future to join our workforce. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law. We will rarely need to rely on your consent to process your personal information.

AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision about that person without any human intervention. We do not currently use automated decision making in our business in relation to applications to join our workforce.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision making unless we have a lawful basis for doing so and we have notified you.

WHO HAS INTERNAL ACCESS TO YOUR PERSONAL INFORMATION?

Your personal information may be shared internally, including with members of the People and Talent (recruitment) teams, managers and senior staff in the business area involved in your recruitment, the technology or legal teams where access to your personal information is necessary for the performance of their roles. We only provide access to your personal information to those of our staff who need to have access to your personal information.

WHO DO WE SHARE YOUR PERSONAL INFORMATION WITH EXTERNALLY?

When using your personal information we may share it with third parties, but we will only do so when it is appropriate and we have a lawful basis for doing so. Third parties that we may share your personal information with include:

- Any third party approved by you.
- Your past employers or referees to obtain references.
- Service or product providers to our business, for example information technology services suppliers, background check providers.
- Third parties that process personal information on our behalf and in accordance with our instructions.
- Another company within our group of companies, especially if you may be working for that part of our group.
- Purchasers, investors, funders and their advisers if we sell all or part of our business, assets or shares or restructure whether by merger, re-organisation or in another way.
- Our legal and other professional advisers, including our auditors or any professional advisors appointed by you, for example a pensions advisor or legal advisor.
- Governmental bodies, HMRC, regulators, police, law enforcement agencies, security services, courts/tribunals.

INTERNATIONAL TRANSFERS

It is sometimes necessary to share your personal information outside of the UK and the European Economic Area (the EEA) or it will be collected outside of the UK and the EEA. This will typically occur when service providers to our business are located outside the EEA or if you are based outside the EEA. These transfers are subject to special rules under applicable data protection laws.

The same applies to any transfer of personal information to another part of our group of companies based outside of the UK and the EEA. We also apply the same standards to any transfer of personal information between members of our group, regardless of where the group company is based.

If we transfer your personal information outside of the UK and/or the EEA, we will ensure that the transfer will be compliant with applicable data protection laws and all personal information will be secure. Our standard practice is to assess the laws and practices of the destination country and relevant service provider and the security measures that are to be taken as regards the personal Information in the overseas location; alternatively, we use standard data protection/contractual clauses. This means that when a transfer such as this takes place, you can expect a similar degree of protection in respect of your personal information.

Our directors and other key staff working for us may in limited circumstances access personal information from outside of the UK and/or the EEA if they are outside of the UK or EEA. If they do so they will be using our security measures and the same legal protections will apply that would apply to accessing personal information from our premises.

In limited circumstances the people to whom we may disclose personal information may be located outside of the UK and/or the EEA and we will not have an existing relationship with them, for example a foreign police force outside of the UK and/or the EEA. In these cases we will impose any legally required protections to the personal information as required by law before it is disclosed.

If you would like any more details about how we protect your personal information in relation to international transfers then please contact our DPO at dpo@gymshark.com.

HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We are committed to keeping your personal information safe and secure and so we have numerous security measures in place to protect against the loss, misuse, and alteration of information under our control. We will always aim to use best in class security systems implemented across our networks and hardware to ensure access and information are protected. Our security measures include:

- Encryption of personal information where appropriate.
- Regular cyber security assessments of all service providers who may handle your personal information.
- Regular planning and assessments to ensure we are ready to respond to cyber security attacks and data security incidents.
- Regular penetration testing of systems.
- Security controls which protect our information technology systems infrastructure and our premises from external attack and unauthorised access.
- Regular backups of information technology systems data with functionality to correct errors or accidental deletion/modification to data.
- Internal policies setting out our information security rules for our staff.
- Regular training for our staff to ensure staff understand the appropriate use and processing of personal information.
- Where we engage third parties to process personal information on our behalf, they do so on the basis of our written instructions, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of personal information.

We take information security very seriously and will use all reasonable endeavours to protect the integrity and security of the personal information we collect about you.

FOR HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION?

We will hold your personal information for the duration of your application process to join us and, if your application is unfortunately unsuccessful, for a further period of up to 3 years after our decision not to take you on. We may, during that period, contact you again to check whether you would still like us to keep you on file for any future positions that may become available and contact you about them if we think you may be suitable for the role. However, in some cases we may need to keep your personal information for longer, for example if it is still relevant to a dispute or legal case or claim.

We will not retain your personal information for longer than necessary for the purposes for which it was collected and for which it is being used.

For more information please contact our DPO at dpo@gymshark.com.

YOUR RIGHTS

As an individual whose personal information we collect and process, you have a number of rights. You may:

- Withdraw any consent you have given to us, although this will only be relevant where we are relying on your consent as a lawful basis to use your personal information, but it is an absolute right. Once we have received notification that you have withdrawn your consent, we will no longer process your personal information for the purpose or purposes for which you originally gave your consent, unless we have another lawful basis for doing so.

- Request details about how your personal information is being used. This right is linked with the right of access mentioned below.

- Request access and obtain details of your personal information that we hold (this is commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal information. This means that you can ask us to delete or stop processing your personal information, for example where we no longer have a reason to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (set out below). The right to have data erased does not apply in all circumstances.

- Object to the processing of your personal information where we are relying on a legitimate interest (ours or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

- Object to direct marketing where we are processing your personal information for direct marketing purposes, for example contacting you about other positions that might suit you. This is an absolute right.

- Request the restriction of processing of your personal information. This enables you to ask us to stop processing your personal information for a period if it is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing your personal information.

- Request the transfer of your personal information to another party in certain circumstances.

- Object to certain automated decision-making processes using your personal information.

You should note that some of these rights, for example the right to require us to transfer your personal information to another service provider or the right to object to automated decision making, may not always apply as they have specific requirements and exemptions which apply to them, and they may not apply to personal information recorded and stored by us. For example, we do not use automated decision making in relation to your personal information. However, some have no conditions attached, so your right to withdraw consent or object to processing for direct marketing are absolute rights.

If you would like to exercise any of these rights, please contact our DPO at dpo@gymshark.com.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person or dealt with by a person who has no right to do so.

Whilst this privacy notice sets out a general summary of your legal rights in respect of personal information, this is a complex area of law. More information about your legal rights can be found on the ICO's website at https://ico.org.uk/for-the-public/.

COMPLAINTS

We hope you don't have any reason to complain, and we will always try to resolve any issues you have, but you always have the right to make a complaint at any time to the ICO if you are based in the UK about

how we deal with your personal information or your rights in relation to your personal information. If you are based outside of the UK you may have the right to complain to your local data protection regulator.

You can make a compliant in writing to the ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, United Kingdom or you can go to https://ico.org.uk/make-a-complaint/.

CONTACTING US

If you have any queries regarding our use of your personal information or this privacy notice then please contact our DPO at dpo@gymshark.com or write to DPO, Gymshark, GSHQ, Blythe Valley Park, 3 Central boulevard, Solihull, B90 8AB, United Kingdom. You can use these details regardless of which of our group companies you are applying to work for.