FMP Global

Marketing & providing Services to b2b clients and contacts under GDPR, and use of 'Legitimate Interest'

Contents

Introduction

FMP Global and its associated subsidiaries are specialist b2b payroll and HR services and software in the UK and internationally with over 40 years of experience. Marketing uses business information for marketing campaigns and data management purposes. Our Payroll Services & Helpdesk, and International HR teams provide professional services. With our dedicated team FMP Global are fully compliant with the requirements as set out in the General Data Protection Regulation ("GDPR").

From 25th May 2018 all businesses in the EU will need to comply with the GDPR which is directly concerned with the collection, storage and use of personal data.

MAY-2018

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

This document addresses the issues most frequently asked and outlines the approach that FMP Global's marketing & services teams have adopted on data processing under GDPR. The following is for information and guidance only – FMP Global would recommend any business also seeks independent legal advice.

Background

The storage and handling of data has for many years been governed by the Data Protection Act 1998 ("DPA") but from May 2018 this will be replaced by the GDPR – which will provide a far more robust set of rules for the collection, storage and processing of personal information. The GDPR is a regulation rather than a directive which means it is a single piece of legislation that applies across all EU member states (and as the UK will still be a member of the EU in 2018 it therefore applies to the UK in the same way). In respect of electronic marketing communications there are additional rules that come from the Privacy and Electronic Communications Regulations 2003 ("PECR"), and with the introduction of the GDPR this is also now in the process of being revised.

What is the impact of GDPR?

Every organisation that holds personal data will be affected by GDPR – that includes personnel records, customer details, sales and marketing prospect information, online identifier data etc. Organisations will be accountable to the data protection supervisory authorities (in the UK this is the Information Commissioner's Office). Whilst the accountability is not a new requirement, GDPR requires all organisations to record and document compliance with all applicable aspects of GDPR. The Regulation gives individuals more rights in respect of their data, including more control and visibility of how their personal data is being used, and the right to have that information removed or moved if requested.

What is Personal Data?

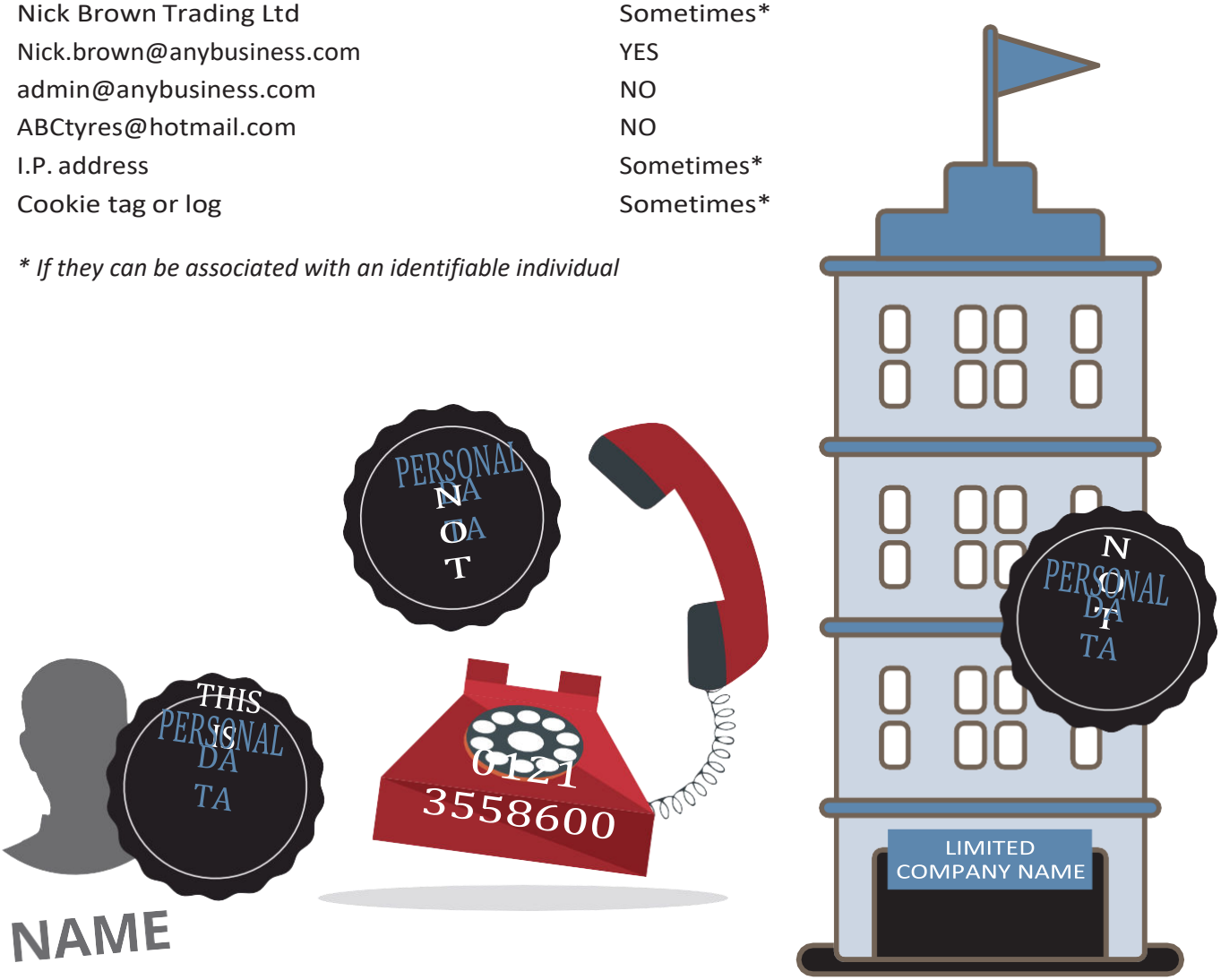
Definition of Personal Data – Article 4(1)

"Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Examples of personal data include elements such as name, address, gender, date of birth, but personal data can also include other less obvious identifiers such as IP addresses. Basically, personal data applies to any data from which a living individual (data subject) could be identified.

Data	Personal Data?
FMP Information Ltd	NO
62 Anchorage Road	NO
Paul Spinks, Managing Director	YES
0121 3558600	NO
ABC tyres (Ltd or not)	NO
Nick Brown Plumbing Services (where company is unincorporated)	YES
Nick Brown Trading Ltd	Sometimes*
Nick.brown@anybusiness.com	YES
admin@anybusiness.com	NO
ABCtyres@hotmail.com	NO
I.P. address	Sometimes*
Cookie tag or log	Sometimes*

** If they can be associated with an identifiable individual*



Lawful Grounds for Processing Personal Data

GDPR is concerned with the collection, storage and processing of personal data – for the use of that data and in respect of electronic marketing communications there are additional rules that come from the Privacy and Electronic Communications Regulations 2003 ("PECR"), and with the introduction of the GDPR this is also now in the process of being revised.

Example	GDPR/PECR
Collecting data	GDPR
Storing data on a database or in a CRM system	GDPR
Processing data (analysing or profiling)	GDPR
Creating a marketing list or campaign list	GDPR
Loading a list into a dialler or email delivery system	GDPR
Sending a mailshot (for B2B)	None
Sending an email or SMS	PECR
Tracking cookies or IP addresses	PECR
Making a phone call	PECR

PECR

There are 6 lawful grounds that can be used for the processing of personal data under GDPR:

1. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
2. Processing is necessary for compliance with a legal obligation.
3. Processing is necessary to protect the vital interests of a data subject or another person.
4. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
5. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)
6. Consent of the data subject.

GDPR

PECR and GDPR

PECR (Privacy and Electronic Communications Regulations) are the rules that relate to electronic marketing communications such as email and SMS. These are in addition to the requirements under the GDPR. (FMP Global do not collect data for the purposes of marketing via SMS so the below relates only to email marketing).

- PECR treats the use of email for marketing communication differently depending on whether it is sent to 'individual subscribers' or to 'corporate subscribers'.

- 'Individual subscribers' include those working for unincorporated entities such as sole traders and partnerships.

- The rules require that electronic mail for direct marketing purposes sent to individual subscribers must be based on a prior consent obtained from such individuals.

- 'Corporate subscribers' consist of those working for companies and other incorporated organisations, such as LLPs.

- PECR allows electronic direct marketing communications to be sent to corporate subscribers (business email addresses of individuals working for incorporated entities) without prior consent, unless the recipient specifically requests not to receive emails from the sender ("opt-out"). Each direct marketing email should include an "unsubscribe" option to allow the individual to notify the sender that he/she no longer wishes to receive emails from the sender.

Legitimate Interest

'The legitimate interests of a controller, including those of a controller to which the Personal Data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller… The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'
Recital 47

Recitals 47 to 50 provide examples of where a controller may have a Legitimate Interest to process data that would also need to be supported via a Legitimate Interest Assessment (LIA).

FMP Global Position

Each legal basis for processing personal data has its own merits and needs to be considered carefully. There is no hierarchy, one legal basis is not 'better' than another, and the ICO advises businesses to examine the most appropriate legal basis for each business.

FMP Global's view is that it is reasonable to rely on legitimate interest as grounds for the processing of personal data for marketing purposes, given the very limited amount of personal information being processed; the fact that it is being used solely for the purposes of marketing to the business for which the individual works and not the individual him/ herself; and that the individuals concerned are likely to be people within the organisation who would expect to be contacted for business communications.

In summary:

- Use of personal data by FMP Global is based on legitimate interest.

FMP Global Process

FMP Global seek to speak directly to businesses to establish whether our payroll and HR services can be used. For payroll services in the UK FMPs bases legitimate interest on the need under PAYE legislation and HMRC rules for employees to be paid, and HR services and software to keep track of those employees. The same principles apply to our international payroll and HR services throughout Europe and the rest of the world. If individuals object (opts-out) to FMP Global storing and using his/her personal data, then the personal data is removed from the FMP Global database. FMP Global use the GDPR compliant Zoho CRM for storing client data and Dotmailer as our primary email system for bulk email. Other systems and software may support this storage.

What does relying on legitimate interest involve?

GDPR requires each organisation to carry out an assessment (and document it) of which lawful grounds for processing of personal data apply to its processing activities.

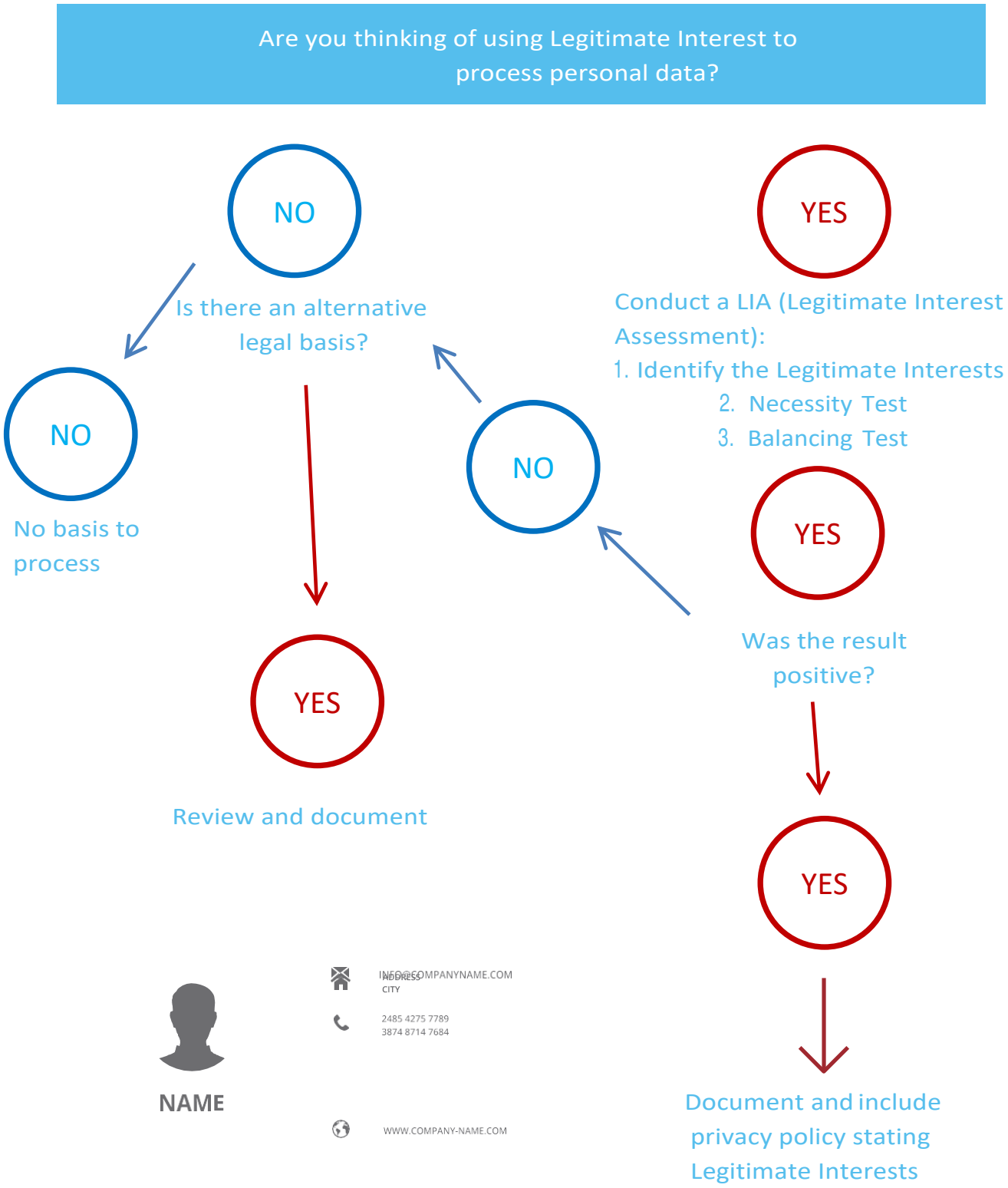
Relying on legitimate interest involves:

1. Establishing the interest of the organisation – for FMP this is promoting goods or services offered us. Processing for direct marketing purposes is specifically mentioned in the GDPR;

2. Carrying out a necessity test – this requires consideration of whether there is another way of achieving the interest, without having to use the personal data. Even if there is another way, but it would require disproportionate effort, the necessity could still be established. You need to consider - is there a way to make direct marketing communication with the correct contacts within an organisation without holding their personal data? It is unlikely that there would be another proportionate way of making direct marketing communications without the necessity to use personal data; and

3. Balancing the interest of the organisation against the fundamental rights of the data subjects and whether the use of their personal data by the organisation could have a significant impact on their fundamental rights. In the context of b2b direct marketing, where communications relate to business services rather than the personal life of the individuals receiving the communications, it is unlikely that the fundamental rights of such individuals would be impaired. Those communications need to be measured and unobtrusive.

The Legitimate Interests Test



If a controller wants to rely on Legitimate Interest the balance between the interests of the controller and the rights of the individual must be considered. To do this a Legitimate Interest Assessment (LIA) must be conducted.

Legitimate Interest Assessment (LIA)

This is a three-stage process:

1 Identify and establish your interest

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

2 Carry out a necessity test.

- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

3 Conduct a balancing test

- What is the nature of your relationship with the individual?
- Would people expect you to use their data in this way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

Legitimate Interest; marketing – What we've concluded

Identifying Legitimate Interests		
Question	Answer	Comments
What is the purpose for processing the data?	To contact UK, European and International businesses to advise them of our payroll and HR services.	
What are your objectives?	All Limited businesses (other than sole trader/ partnerships) need a way to be able to pay their employees. FMP provide HMRC approved services and software to those companies to be able to comply with UK law.	
Who benefits from the processing?	The employee processing payroll may see that there is an alternative way of processing, and identify HR tools that could help them control employees.	
What is the importance of those benefits?	It could save the company in terms of administrative time, money, or the need to retain specialist knowledge. Outsourcing payroll, or the provision of HR services, can help with transition of a business to the next level in terms of strategy and tactical execution.	
What is the impact of not being able to proceed with the processing?	The business we are approaching could carry on but may ultimately have pressure that could impact on staff morale, retention, compliance with legislation and ultimately fines/ business failure.	

Necessity Test		
Question	Answer	Comments
List the reasons the processing is important to the data controller?	Email forms the simplest way of communicating with a potential client. FMP marketing use data collected from downloads and contact forms from our website (where it is reasonable under Legitimate Interest to suggest that individuals working on behalf of companies are interested in our products and services), contacts at industry events and seminars where they approach our staff on stand, and bought data lists from auditable suppliers (we currently use a GDPR compliant 118 subsidiary), existing client data. Without relevant contact data we	

	would be unable to identify which contacts within a business are responsible for HR and Payroll – a key factor of GDPR. The processing allows us to input into Dotmailer, an industry leading email management system. The data is checked and suppressed against a global suppression list and cleaned before use, maximising opportunity to eliminate those contacts that have registered against the CTPS database and protecting client information. Bought data (from leading data house 118 group) similarly is scrutinised against CTPS and GDPR tested. The Dotmailer system automatically checks that emails are GDPR compliant, by automatically checking that 'Unsubscribe' is recorded on all outbound emails, and if clicked, automatically removing client contact details from the database, ensuring the privacy of data.	
Is this a reasonable way to process data?	Yes. Email is an easy and controlled method of contact. Using Dotmailer we could control how data is used, protecting b2b client information in a way that allows easy and instant ability to be removed. We have investigated the situations fully, gaining an in depth understanding of the legal position, and seeking guidance from Dotmailer, our email provider and our bought data providers.	
Is there an alternative way to achieve the same results?	We could and do send mail by post, but this is more of a scatter gun approach. We have little understanding of whether the information sent is acceptable to a b2b client. Use of data in this way will be both ethical and lawful.	

Balancing Test

Question	Answer	Comments
What is your relationship with the subject?	B2B market contacts – we seek to identify relevant legitimate contact primarily with 'payroll' 'Finance' or	

	'HR' in their title, or in director level positions within smaller companies where it is likely that they will have ownership of the payroll function. People would expect their data to be used in this way.	
Is any of the data 'sensitive'?	At marketing stage there is no sensitivity. At this level we hold basic company information and the name, job title and email address.	
Would the data subject expect their data to be used in this way?	Yes.	
Might the data subject object or find the processing intrusive?	Possibly if they are not responsible for HR or Payroll within their business, but our email contains the relevant opportunity to unsubscribe, thus mitigating any risk of intrusion. The automatic nature of the unsubscribes ensures there is no human element involved in the unsubscribe.	
What is the possible impact on the individual?	Nominal. As these are to work related email addresses they can use appropriate systems to unsubscribe as needed.	

Services

FMP Global may provide you with a number of services, or software solutions. We may use your employees' data to enable us to process and pay your payrolls, to report to HMRC and pension providers, to advise on HR matters, and to administer employee benefits programmes as necessary.

We will process the data in line with GDPR privacy and security expectations and guidelines. There will be a formal, contractual agreement between the Client and FMP Global which details the nature and parameters of the processing.

Payroll Bureau & International Payroll and HR Processing.

We will collect and process the data in line with the principles of GDPR. We act as a data processor for payroll and HR data and will process the data to ensure compliance to statutory payroll requirements and the data controller's specified purpose.

We process the data in line with contractual requirements and obligations for all our clients.

The data is collected, transmitted and processed securely, in line with our stringent ISO 27001:2013 processes.

We will process the data fairly and avoid over processing of the data. As an example, the list of fields below represents the data required for a successful HMRC RTI submission.

Employee Information
National Insurance number
Title
Surname or family name
Forename or given name
Second forename or given name
Initials
Date of birth
Gender
Address
UK postcode
Foreign country
Payroll ID
Payroll ID changed indicator
Old payroll ID for this employment
Irregular payment pattern indicator
Pay and deductions
Taxable pay
Tax deducted or refunded
Student Loan deductions recovered
Pay after statutory deductions
Deductions from net pay
On strike
Non-tax or NIC payment
Student Loan Plan type

Year to date totals
Taxable pay to date
Total tax to date
Total Student Loan repayment recovered to date
If you've employed the same person more than once in a tax year, report for their current employment only.
Pension deductions
Employee pension contributions paid under 'net pay arrangements'
Employee pension contributions not paid under a 'net pay arrangement'
Employee pension contributions paid under 'net pay arrangements' year to date
Employee pension contributions not paid under a 'net pay arrangement' year to date
Statutory maternity, paternity, adoption and shared parental pay
Statutory Maternity Pay (SMP) year to date
Statutory Paternity Pay (SPP) year to date
Statutory Adoption Pay (SAP) year to date
Statutory Shared Parental Pay (ShPP) year to date
ShPP: Partner surname or family name
ShPP: Partner forename or given name
ShPP: Partner second forename or given name
ShPP: Partner National Insurance number
If you pay benefits through payroll
Items subject to Class 1 National Insurance only
Benefits this period taxed via payroll
Benefits taxed via payroll year to date
Employee pay information
Employee tax code
Employee tax code: Week 1/Month 1 indicator
Employee hours normally worked
Pay frequency
Payment date
Tax week number
Tax month number
Number of earnings periods covered by payment
Bacs hash code
Aggregated earnings indicator
National Insurance
National Insurance category letter
Gross earnings for NICs in this period
Gross earnings for NICs year to date
Earnings at the Lower Earnings Limit (LEL) year to date

Earnings above LEL up to and including the Primary Threshold (PT) year to date
Earnings above the PT, up to and including the Upper Accrual Point (UAP) year to date
Earnings above the UAP, up to and including the Upper Earnings Limit (UEL) year to date
Employee contributions payable this period
Employee contributions payable year to date
Total of employer's contributions payable in this pay period
Total of employer's contributions payable year to date
Scheme Contracted Out Number (SCON)
Report this National Insurance information when you pay a director.
Director's NIC calculation method
Week of director's appointment
When an Employee Joins
Start date
Starter declaration
Student Loan indicator
Address
UK postcode
Foreign country
Passport number

Third Parties

We use robust contractual provisions to protect the storage and transfer of personal data when dealing with external and internal partners. We are updating these in line with the GDPR. FMP protects EU personal data transferred outside of the EEA using standard contractual clause language, where appropriate, and other EU approved mechanisms such as Privacy Shield for transfers to third party business partners in the USA who have registered to that scheme.

Data Retention Policy

Data relating to payroll processing will be kept for a period of time. At the end of that period, you will be contacted and given the option to either purchase additional storage or confirm the secure erasure of the data. If the data is paper based, it will be securely shredded.

HR & Payroll Software – GDPR Advice to clients using our software

We will collect and process our client's data in line with GDPR due to our contractual obligations to provide software systems and support surrounding the systems. You act as the data controller and processor; therefore, the onus is on you, the client to ensure the necessary contracts are in place to ensure your GDPR compliance.

It is our clients' responsibility to ensure the completeness, accuracy and integrity of the data. Our Consultants will setup, configure and train your users on your chosen software.

We will use dummy data to train your staff, unless you request that we train you on your data. When we do train you on your system, it is your responsibility to ensure that the necessary security, data

segregation and privacy is in place for the users being trained.

Any data sent to our Helpdesks in order to resolve an outstanding support issue will be transmitted and processed, in line with GDPR. Data will be stored securely and retained in line with our data retention policy.

Self Service Portals

Whereby a client has purchased our self-service portals, it is the client's responsibility to ensure that the self-service portal is accessibly only via password for each employee. The passwords allocated should not be generic and each password should be unique.

E-Payslips

It is the client's responsibility to ensure that the e-payslips are password protected. The passwords should not be generic, and each password should be unique.

Ensuring our support teams are GDPR compliant

As part of our support investigations, in order to try and investigate / resolve an outstanding support query, our Helpdesks may request data backups.

The backup files are transmitted and stored securely on our servers, we have taken additional security measures to ensure we are fully GDPR compliant.

Any data transmitted to us is held on centralised, secure servers and managed in line with our data retention policy.

Hosted System clients

Our service provider, 6 degrees, is GDPR compliant and hold a number of security ISO certifications. Further details can be found here; https://www.6dg.co.uk/statement-gdpr-compliance-2/

FAQ

Q: Will FMP be sending me a new contract with GDPR language?

A: We are reviewing our existing contractual relationships, and existing templates, these will be updated and re-issued, in line with GDPR requirements. We may provide new language where we deem it is required.

Q: Can I see a copy of policies and procedures?

A: Our policies and procedures at FMP Global are confidential and we do not share them with external parties. We do our best to provide our clients with relevant information in other ways, such as providing this fact sheet, and educating our staff on our compliance programs.

Q: Can I have more information about your information security protocols?

A: We will only share limited information on our security protocols due to the importance of maintaining confidentiality.

Q: Who do I contact for more information?

A: You should contact your primary day to day contact at FMP Global if you want more information and he or she will manage the request through our internal processes

Q. Will there be a change in how data is transmitted to and from FMP Global?

A: There is likely to be a change and we hope to have details of this out to all our clients as soon as possible. We are looking at a solution with minimal disruption for all.

Q: Does the Employer need to seek permission or consent from the employees to share their data with our payroll bureau?

A: No, you do not need each individual employee's consent, as you are legally obliged to pay staff. You will, however, need to advise them that you are sharing their information with a 3rd party.

Privacy Policy

This page aims to help you understand what information we might collect about you and how we use it.

FMP Global is the Data Processor and operates through several companies within our group & with contract third-parties, which will also be data controllers in respect of your personal data. Our group companies are as follows: FMP Global (incorporating Eurowage Ltd, FMP Payroll Services Ltd, FMP HR & Payroll Software Ltd, MCN Associates Ltd) and these companies are registered with the Data Protection Register (ZA290393 / ZA290366 / Z1115288 / ZA024069), and are ISO certified (9001/27001/14001/22301)

FMP Global is committed to protecting and respecting your privacy and will comply with the applicable data protection laws in all our dealings with your personal data.

We may collect and process the following data about you:

- Information about you, such as your name, your business telephone number and email address
- Information that is provided by filling in forms on our sites. This includes information provided at the time of downloading gated material such as eBooks, brochures or case studies associated with HR and payroll, or completing a contact form or subscribing to newsletters;
- If you contact us, we may keep a record of that correspondence;
- We may also ask you to complete surveys that we use for research purposes, although you do not have to respond to them;
- Details of your visits to our site and emails received including, but not limited to, traffic data, location data, weblogs and other communication data, whether this is required for our own billing purposes or otherwise.

IP addresses

We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration and to report aggregate information to our partners, sponsors or advertisers. This is statistical data in aggregated form about our users' browsing actions and patterns and will not allow our partners to identify you from such data.

Use of Cookies

What is a Cookie? Cookies are small, unique strings of code stored on your computer to improve your use of our sites and to help us to improve functionality and security of the sites. We use both session and persistent cookies; session cookies expire when you close the browser and persistent cookies remain on your computer until you remove them. We may also use cookies to automatically collect information from your computer when you visit our sites, and automatically store it in the log files. This may include information on type of browser software, website activity and your IP address.

Cookies enable us to:

Estimate our audience size and usage pattern

Allow us to customise our site according to your individual interests
Speed up your searches
Allow you to more easily find previously viewed content

You can refuse to accept all or some cookies by modifying settings within your browser (for guidance on how to do this visit http://www.aboutcookies.org/). However, if you block the session cookies you may be unable to access certain parts of our sites.

Where we store your personal data

The data that we collect from you may be transferred to, and stored at, a destination outside the United Kingdom and the European Economic Area ("EEA"). It may also be processed by staff operating outside the UK or the EEA who work for us or for one of our suppliers. We will take all steps reasonably necessary to ensure that any personal data transferred outside the UK or the EEA is treated securely and in accordance with the applicable data protection laws.

We will store all information about you on secure servers. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site. Each business unit has conducted its own security reviews in relation to data transmission and has adjusted its processes accordingly. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Legal basis to process your personal data

Under the applicable data protection laws, we need a lawful basis to collect and use your personal data. The law allows for six lawful bases to process people's personal data, and one of them allows personal data to be legally collected and used if it is necessary for a legitimate interest of the organisation – if it is fair and balanced and does not unduly impact the rights of individuals.

Due to the nature of our business it is not practical for us to ask every individual for his/her consent. We have assessed our and our clients' business interests in carrying out marketing activities and we have carefully considered the impact the collection and use of personal data could potentially have on individuals' rights. Our databases contain business data, which is used to promote HR and Payroll business in the UK and such activities are unlikely to affect the fundamental rights and freedoms of individuals concerned. We have therefore concluded that the most appropriate lawful ground for the processing of your personal is 'legitimate interest', in your capacity as representative of your company (b2b)

In the event you request any goods and/or services from us, we will rely on our contractual relationship to process your personal data to provide such goods and/or services to you. In certain very limited circumstances we may also rely on a specific consent provided by you for the processing of your personal data. In those circumstances you can withdraw your consent at any time by contacting us – see our contact details below.

Uses made of the information

We may use information held about you in the following ways, to:

- Ensure that content from our site is presented in the most effective manner for you and for your computer;
- Provide you with information, products or services that you request from us or which we feel may interest you;
- Carry out our obligations arising from any contracts entered into between you and us;
- Allow you to participate in interactive features of our service, when you choose to do so; and
- To notify you about changes to our service.

When contacting you for the above purposes we may do so by phone, post, email or other electronic means, unless you tell us otherwise.

We may share information, including personal data, with third parties that provide support to our business

Data Retention

We collect and store personal data for our business database. As such, we will only retain your personal data for as long as we believe it is up-to-date, i.e. as long as it is associated with a business that is included in our database. We verify our data periodically and if we learn that you are no longer involved with a business that is in our database, we will remove your data from our records.

Additional Information

If you have any concerns or complaints about our privacy activities, you can contact us on dpo@fmpglobal.com. You can also contact the Information Commissioner's Office on 0303 123 1113 (www.ico.org.uk).

Changes to Our Privacy Policy

Any changes we may make to our privacy policy in the future will be posted on this page and, where appropriate, notified to you by e-mail.

Contact

If you have any questions, comments and requests regarding this privacy policy please contact us dpo@fmpglobal.com

Cookie Policy

FMP Global is the data controller of your personal data. We operate through several companies within our group, which will also be data controllers in respect of your personal data. Our group companies under the FMP Global group include Eurowage Ltd, FMP Payroll Services Ltd, FMP HR & Payroll Software Ltd, and MCN Associates Ltd

FMP Global is committed to protecting and respecting your privacy and will comply with the applicable data protection laws in all our dealings with your personal data.

We use cookies and similar technologies (herein referred to in general as "cookies") for a variety of purposes on our websites or when we send you an email. Cookies are small files that are stored on your browser when you visit a website. The main purpose is to keep a record of your visit, time spent on the site, pages visited, and searches made. We may also use cookies to automatically collect information from your computer when you visit our sites, and automatically store it in the log files. This may include information on type of browser software, website activity and IP address.

The main purposes of the cookies we use are:

Session – to allow the user to navigate our sites more easily; for example, you don't have to go in as a new user every time.
Analytics – to improve the user experience of the site by providing statistics on how the site is used.
Tracking – we may use cookies hosted by third parties which allow for an improved site experience by collecting data such as browser, IP address, pages visited, content viewed, timing of visits and clickstream data. When you visit our websites or open an email we have sent, we or one of our third-party partners may place a cookie on your browser.

How to refuse and delete cookies

You can refuse to accept all or some cookies by modifying settings within your browser - for help on how to do this visit www.aboutcookies.org.uk

You may also delete all cookies on your browser – click help on your browser or visit www.aboutcookies.org.uk

Please remember that if you block the session cookies you may be unable to access certain parts of our sites.