

## Privacy Notice Compliance Checklist

### Information to be provided where personal data are collected from the data subject and at the time of collection

Item	Article 13	Assessment
The <b>identity and contact details</b> of the data controller.	1 (a)	Compliant if Constellium UK Ltd is the controller for all employee personal data. If Constellium Group companies also control employee personal data then this should be amended. "Constellium UK Ltd., with registered office in Greenville Court, Britwell Road, Burnham, Slough SL1 8DF, United-Kingdom, collects some of your data"
The identity and contact details of our <b>representative</b> within the EU (if the data controller is not within the EU).	1 (a)	n/a
The contact details of the <b>data protection officer</b> (if the data controller is required to have one).	1 (b)	Constellium UK Ltd has not appointed a Data Protection Officer to date. I doubt the company' core activities require large scale systematic monitoring, processing large scale of special categories or criminal convictions as per GDPR article 37, and therefore do not expect that it requires a DPO.
The <b>purposes of the processing</b> for which the personal data are intended.	1 (c)	Compliant. "Management of our legal obligations (social and tax declarations, storage of legal documents, management of pension); - Management of the performance of your employment contract (payment of your remuneration, management of training, management of business expenses and corporate cards, management of company cars etc.); - Internal communication (intranet; phone directory); - Use of IT tools of the company."
The <b>lawful basis</b> for the processing purposes above.	1 (c)	Compliant. "This processing is necessary for the performance of your employment contract as well as for the respect of our legal obligations." The records of processing activities at present include these only for Constellium UK: <ul style="list-style-type: none"> <li>• Amex corporate card</li> <li>• Company car</li> <li>• Company mobile phone</li> <li>• Health insurance</li> <li>• Life cover and permanent health cover</li> <li>• Payroll</li> <li>• Pension</li> </ul>

		Note: it is possible that some other processing activities are, or will be, undertaken on the basis of legitimate interest; if so we should amend this.
If legitimate interest is the legal basis, what the <b>legitimate interest</b> pursued by the controller or a third party is.	1 (d)	n/a
The <b>recipients</b> or categories of recipients of the personal data (if any that are external to the data processor).	1 (e)	Not compliant. Constellium UK Ltd shares personal data with suppliers (Eacotts at least, possibly others) and so we should amend this to include categories of recipients: (i) Accountants, (ii) External HR Advisors (iii) any other categories.
The details of <b>transfers</b> of the personal data to any third countries or international organisations and details of any adequacy decision by the EU Commission or reference to appropriate or suitable safeguards.	1 (f)	Compliant if Constellium UK Ltd does not transfer personal data outside the EU.
The <b>period</b> for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.	2 (a)	Compliant. "We keep these data for a maximum period of 6 tax years as of the end of your employment contract."
The existence of the right to request from the controller <b>access</b> to personal data.	2 (b)	Compliant. "In application of articles 16 to 21 of the GDPR and under the strict conditions specified by them, you have the right to object and to restriction to the processing as well as a right of access, rectification, erasure and portability of your data."
The existence of the right to request from the controller <b>erasure</b> of personal data	2 (b)	Compliant. See above
The existence of the right to request from the controller <b>rectification</b> of personal data.	2 (b)	Compliant. See above
The existence of the right to request from the controller <b>restriction</b> of processing concerning the data subject.	2 (b)	Compliant. See above
The existence of the right to <b>object</b> to the processing.	2 (b)	Compliant. See above
The existence of the right to data <b>portability</b> .	2 (b)	Compliant. See above Although note that data processing is probably not carried out by automated means so the right under GDPR article 20 does not apply.
The right to <b>withdraw consent</b> (if processing is under Art 6 (1) (a) or 9 (2) (a) without affecting the lawfulness of processing before any withdrawal.	2 (c)	n/a
The right to lodge a <b>complaint</b> with a supervisory authority.	2 (d)	Compliant. "In case you cannot exercise the aforementioned rights, you can lodge a complaint to the Information Commissioner's Office ( <a href="https://ico.org.uk/">https://ico.org.uk/</a> )."

The details of whether individuals are under a <b>statutory or contractual obligation to provide the personal data</b> and the possible consequences of a failure to provide it (if applicable)	2 (e)	Not Compliant. We rely on contractual necessity and legal obligation so employees are obligated to provide some personal data or we will be unable to employ them.
The existence of automated <b>decision-making</b> , including <b>profiling</b> , referred to in Art 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	2 (f)	n/a