

Data protection

Privacy Policy

We are delighted that you are using our application SmartBlue and shown an interest in our company and products. In accordance with the relevant data protection regulations, we are providing you with the following information regarding which personal data we collect when you use our application, the purposes for which we use this data, and how we utilize it to optimize our services for you.

A. General information

1. Responsible entity and data protection officer

Hereinafter you find information about the company responsible for processing your data, the data protection officer, as well as the relevant regulatory body.

Responsible Company

Endress+Hauser Process Solutions AG
Christoph-Merian-Ring 12
4153 Reinach BL

Data Protection Officer

Felix Kraft
E-Mail: felix.kraft@endress.com
Phone: +41 61 715 7323

Federal Data Protection and Information Commissioner

Adrian Lobsiger
Feldegweg 1
3003 Bern

<https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/the-commissioner.html>

2. Type of data processed, the purpose and legal basis

SmartBlue tracks certain user behavior related around crash logging as well as user interaction. This information is used as feedback for us to see how the SmartBlue app is used and how it can be improved in the future with additional features or UI alterations.

The tracking of user information can be deactivated at any time within the settings menu of SmartBlue. You will also be informed of tracking upon first running of the SmartBlue app where you will have the option to disable the functionality.

2.1 Crash Tracking

The SmartBlue Mobile Application uses the crash reporting tool, Crashlytics a business division of Google inc. The application is used to send our developers further information related to crashes and potentially bugs within our application.

The Services automatically collects certain information that does not personally identify End Users who access or use mobile applications that use the Services. This includes:

- Location Information
- Mobile Device Module information
- Identified crash logs

Location Information — Location (on a country level) is collected and shared with Crashlytics to provide us with anonymous analytical information about our users and visitors. We do not track precise information related to location.

Device and Crash Log information — Device and usage information will be shared with Crashlytics to determine the type of phone, the OS version of the phone and the crash log information

The legal basis for processing the data above is our legitimate interest (Article 6(1f) GDPR for the EU).

Last revised: 05.05.2020

2.2 User Behavior Tracking

SmartBlue does not track any personal information such as username and password of field devices, any field device settings or any parameter values that have been configured. Any assets such as PDF reports, generated videos etc. are also never stored or tracked by Endress+Hauser.

SmartBlue tracks the following User Events using Google Firebase, in the event there is a valid internet connection:

- The type of field device that has been logged into
- The serial number and firmware number of the field device that has been logged into
- The amount of times certain field device parameters have been set
- The amount of jumps from SmartBlue to the Operations App
- The amount of times a certain module has been opened with the SmartBlue App (e.g. Envelope Curve, Create Documentation etc.).
- The amount of times a type of Wizard has been selected
- The amount of times a Demo Device has been opened

The legal basis for processing the data above is our legitimate interest (Article 6(1f) GDPR for the EU).

3. Your rights

If the processing of your personal data falls within the scope of the GDPR, you have the following rights, otherwise the statutory provisions applicable to the processing apply.

If your personal data is processed, you are a data subject, as defined by GDPR. Accordingly, you have the following rights vis-à-vis us as the responsible entity. If you wish to exercise your rights or obtain further information, please contact us or our data protection officer:

a) Rights pursuant to Article 15 et seq. GDPR

(1) The data subject has the right to request confirmation from the responsible entity as to whether personal data concerning the subject is processed and, if so, the subject has a right to **information** about this personal data and to the details specified in Article 15 GDPR. Under certain statutory conditions you have the right to **rectification** under Article 16 GDPR, the **right to restriction of processing** under Article 18 GDPR and the **right to erasure** ("right to be forgotten") under Article 17 GDPR. Furthermore, you have the right to receive the personal data in a structured, commonly used, machine-readable format (**right to data portability**) under Article 20 GDPR, provided that processing is automated and based on consent in accordance with Article 6(1a) or Article 9(2a) or on a contract in accordance with Article 6(1b) GDPR.

b) Withdrawal of consent in accordance with Article 7(3) GDPR

If processing is based on consent, you may at any time withdraw the consent you gave us to process personal data. Please be aware that withdrawal of consent has future effect only. It has no effect on processing based on consent before its withdrawal.

c) Right to lodge a complaint

You have the option to send a complaint to us or to a data protection regulatory body (Article 77 GDPR). On this website you can find information about the company responsible for processing your data, the data protection officer, if applicable, and the relevant regulatory body.

d) Right to object under Article 21 GDPR

In addition to the rights mentioned above, you have the right to object, as follows:

Last revised: 05.05.2020

(1) Right to object on a case-by-case basis

You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data which is based on Article 6(1e) GDPR (data processing in the public interest) and Article 6(1f) GDPR (data processing on the grounds of the balance of interests); this includes any profiling on the basis of this provision, as defined in Article 4(4) GDPR.

We will cease processing your personal data if you lodge an objection, unless we can provide compelling legitimate reasons for doing so which outweigh your interests, rights and freedoms, or unless the processing is used for the purposes of asserting, exercising or defending legal claims.

(2) Right of objection to the processing of data for advertising purposes

In individual cases, we process your personal data for direct marketing purposes. You have the right to object at any time to the processing of personal data for the purposes of such marketing; this includes profiling insofar as it is related to such direct marketing. If you object to processing aimed at direct marketing, we will cease processing your personal data for such purposes.

4. General information (disclosure of data to third parties)

(1) Your personal data will not be sold, disclosed or otherwise disseminated to any third party without your express consent, except in cases specified in this Privacy Policy.

(2) Within the responsible Endress+Hauser company, those persons who need your data in order to fulfill our contractual and statutory duties, or safeguard legitimate interests, are granted access to it. Furthermore, companies affiliated to the Endress+Hauser group, service providers and vicarious agents employed by us, and public authorities or third parties may receive data for such purposes. Service providers and vicarious agents, etc. authorized by us are contractually obliged to comply with relevant data protection laws.

5. Security

(1) We have put in place technical and organizational security measures (in accordance with Article 24 and Article 32 GDPR for the EU) in order to protect your personal data against loss, destruction, manipulation and unauthorized access. All of our staff and all third parties involved in data processing are obliged to comply with relevant data protection laws and treat personal data confidentially.

6. Changes to our privacy provisions

We reserve the right to make changes to our security and data protection measures to the extent necessary due to technological advances or changes in law. In such cases, we will also amend our Privacy Policy accordingly. Therefore, please take into account the latest version of our Privacy Policy.

数据保护

隐私政策

看到您正在使用我们的应用程序 **SmartBlue**，且对我们的公司和产品比较感兴趣，我们感到非常高兴。根据相关数据保护法规的规定，我们会为您提供以下信息，内容涉及我们会在您使用我们应用程序时收集哪些个人数据、我们使用这些数据的目的以及我们如何利用这些数据来优化我们为您提供的服务。

A. 基本信息

1. 责任实体和数据保护官

在下文中，您可以了解到负责处理您数据的公司、数据保护官以及相关监管机构的信息。

责任公司

Endress+Hauser Process Solutions AG
Christoph-Merian-Ring 12
4153 Reinach BL

数据保护官

Felix Kraft
电子邮箱: felix.kraft@endress.com
电话: +41 61 715 7323

联邦数据保护与信息专员

Adrian Lobsiger
Feldeggweg 1
3003 Bern

<https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/the-commissioner.html>

2. 处理数据的类型、目的及法律依据

SmartBlue 可跟踪与崩溃记录日志和用户交互相关的某些用户行为。这些信息可用作反馈信息，以便我们了解 **SmartBlue** 应用程序的使用情况以及将来如何通过其他功能或 UI 更改来对其进行改进。

您可以随时在 **SmartBlue** 的设置菜单中取消对用户信息的跟踪。您还将在首次运行 **SmartBlue** 应用程序时收到跟踪通知，此时您便可以选择禁用该功能。

2.1 崩溃跟踪

SmartBlue 手机应用程序使用的是谷歌公司业务部门的崩溃报告工具 **Crashlytics**。该应用程序用于向我们的开发人员发送与应用程序内的崩溃和潜在漏洞相关的更多信息。

这些服务会自动收集某些信息，但无法通过这些信息确定访问或使用这些服务的移动应用程序的最终用户之身份。这些信息包括：

- 位置信息
- 移动设备模块信息
- 确定的崩溃日志

位置信息——收集（国家层面）位置信息，并与 **Crashlytics** 共享，以向我们提供有关用户和访问者的匿名分析信息。我们并不追踪与位置相关的精确信息。

设备和崩溃日志信息——设备和使用情况信息将与 **Crashlytics** 共享，以确定设备的类型，设备的操作系统版本以及崩溃日志信息。

处理上述数据的法律依据是我们的合法权益（欧盟《通用数据保护条例》（GDPR）第 6(1f) 条）。

最后修订：2020 年 5 月 5 日

2.2 用户行为跟踪

SmartBlue 不会跟踪任何个人信息，如现场设备的用户名和密码、任何现场设备设置或已配置的任何参数值。Endress + Hauser 也永远不会存储或跟踪 PDF 报表、生成的视频等任何资产。

如果存在有效的互联网连接，则 SmartBlue 会使用谷歌的 Firebase 跟踪以下用户事件：

- 已登录的现场设备的类型
- 已登录的现场设备的序列号和固件编号
- 设置某些现场设备参数的次数
- 从 SmartBlue 跳转到 Operations 应用程序的次数
- 使用 SmartBlue 应用程序打开某个模块的次数（例如，包络曲线、创建文档等）。
- 选择一种类型向导的次数
- 演示设备被打开的次数

处理上述数据的法律依据是我们的合法权益（欧盟《通用数据保护条例》（GDPR）第 6(1f)条）。

3. 您的权利

若您的个人数据处理在 GDPR 规定的范围内，则您拥有以下权利，否则，您需遵守适用于个人数据处理的法律条款。

如果您的个人数据被处理，那么您便是 GDPR 定义的数据主体。因此，作为责任实体，相对于我们，您享有以下权利。如果您希望行使自己的权利或获取更多信息，请联系我们或我们的数据保护官：

a) GDPR 第 15 条及其后条款规定的权利。

(1)数据主体有权要求责任实体确认是否已处理与该主体有关的个人数据，如果已处理，则该主体有权获取有关此个人数据的**信息**以及 GDPR 第 15 条规定的详细信息。在某些法定条件下，您根据 GDPR 第 16 条享有进行**更正**的权利，根据 GDPR 第 18 条享**有限制处理**的权利，以及根据 GDPR 第 17 条享有**删除**的权利（“被遗忘的权利”）。此外，您有权按照 GDPR 第 20 条的规定，以结构化、常用、机器可读的格式（**数据可携性权利**）接收个人数据，但前提是数据处理自动进行，并且数据处理要符合根据 GDPR 第 6(1a)条或第 9(2a)条制定的同意书或遵守根据 GDPR 第 6(1b)条订立的合同。

b) 根据 GDPR 第 7(3)条撤回同意书

如果处理基于同意书执行，您可随时撤回您赋予我们处理个人数据的同意书。但请注意，撤回同意书仅对未来有效。撤回同意书对撤回之前基于同意书执行的处理没有影响。

c) 提出控诉的权利

您可以选择向我们或数据保护监管机构投诉（GDPR 第 77 条）。在此网站上，您可以了解到负责处理您数据的公司、数据保护官（若适用）以及相关监管机构的信息。

d) GDPR 第 21 条规定的异议权

除上述权利外，您还有以下异议权：

(1) 根据具体情况提出异议的权利

您有权基于与您的特定情况有关的理由，随时对根据 **GDPR 第 6(1e)条**（符合公共利益的数据处理）和 **GDPR 第 6(1f)条**（基于利益平衡的数据处理）处理您的个人数据提出异议；包括在 **GDPR 第 4 条第(4)款**中定义的基于此条款的任何分析。

如果您提出异议，我们将停止处理您的个人数据，但我们若能够提供超过您的利益、权利和自由的令人信服的合理理由，或者将处理用于主张、行使或捍卫法定求偿权的目的则除外。

(2) 就出于广告目的处理数据提出异议的权利

在个别情况下，我们会出于直接营销目的处理您的个人数据。您有权随时就出于此类营销目的而处理个人数据提出异议；包括与这种直接营销有关的分析。如果您反对以直接营销为目的的数据处理，我们将停止出于此类目的处理您的个人数据。

4. 一般信息（向第三方披露数据）

(1) 未经您的明确同意，您的个人数据不会出售、披露或以其他方式散布给任何第三方，但本隐私政策中规定的情况除外。

(2) 在负责任的 **Endress + Hauser** 公司内，那些为履行我们的合同和法定职责或维护合法利益而需要您的数据的个人，均可获取此类数据。此外，隶属于 **Endress + Hauser** 集团的公司、我们雇用的服务提供商和代理机构、政府机构或第三方可能会出于此类目的接收相关数据。我们授权的服务提供商和代理机构等在合同层面上具有遵守相关数据保护法律的义务。

5. 安全

(1) 为保护您的个人数据免于丢失、破坏、操纵和未经授权的访问，我们已根据欧盟 **GDPR 第 24 条**和 **第 32 条**采取技术和组织安全措施。我们参与数据处理的所有的员工以及所有第三方均有义务遵守相关数据保护法律，并对个人数据进行保密。

6. 我们隐私条款的变更

我们保留因技术进步或法律变更而在必要的范围内对我们的安全和数据保护措施做出改变的权利。在这种情况下，我们也将相应地修改我们的隐私政策。因此，请顾及我们最新版本的隐私政策。