交大法學評論，第 11 期，頁 135（2022）

論德國科技防疫措施下之個資風險與保護法制

彭睿仁*

摘　要

自 2020 年 3 月初起，新冠肺炎（COVID-19）確診案例每日在德國各邦大量增加。為有效減緩疫情惡化，德國國會分別於同年 3 月及 5 月快速通過「全國範圍流行病情勢下之國民保護法」（Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite）及「全國範圍流行病情勢下之國民保護法第二次法案」（Das Zweite Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite），以及該法對「傳染病防治法」（Infektionsschutzgesetz, IfSG）等法律條文修正後之授權。其中，增修後之「傳染病防治法」（IfSG）第 4 條及第 14 條，授權防疫機構「羅伯特科赫研究所」（Robert Koch-Institut, RKI）研發「德國電子通報資訊系統」（Deutsches Elektronisches Melde- und Informationssystem für den Infektionsschutz, DEMIS），以投入病毒感染追蹤及防止擴散之用。而此一系統即為德國聯邦衛生部（Bundesministerium für Gesundheit, BMG）及「羅伯特科赫研究所」開發並推動之「新冠病毒警示追蹤 App」（Corona-App）。

在民眾自願安裝後，App 透過行動裝置定位及接觸資料回傳防疫主管機

* 國科會科技辦公室政策協調組副組主任、東吳大學政治學系兼任助理教授；德國科隆大學經濟暨社會科學博士。

投稿日：2021 年 1 月 14 日；採用日：2021 年 12 月 13 日

關主機，即時追蹤用戶特定距離內是否接觸確診者與其移動足跡。回傳資料經分析後，可快速篩選出與確診者之可能接觸者，並即刻召回、隔離及匡列下一波可能接觸者。App 用於防疫雖有法源，但其實際應用仍造成德國法學及公衛學界之爭議。因 App 執行時所蒐集的敏感及一般個資，均傳送行政機關進行處理，難以排除個資濫用對人格權及隱私權造成侵害之疑慮。

對此，反對者認為，App 雖係自願使用，但個資蒐集種類、範圍及處理方式並無法律明文，不宜貿然推行。但支持者卻認為，資料保護過度及應用過於保守，才會違反個人「健康完整無缺」之基本人權。正、反意見間雖各有論據，但無共識。對此，本文將從歐盟《一般資料保護規則》（GDPR）及德國相關國內法之觀點，探討德國政府採用追蹤 App 等科技工具進行防疫之適法議題及後續涉及之人權爭議，並以研析結果，解釋相關法律爭議之解決途徑，作為日後研究相關防疫法制之重要參考。

關鍵詞：傳染病防治法、追蹤 App、GDPR、敏感個資保護、確診足跡追蹤

Cite as: 11 NCTU L. REV., September 2022, at 135

Risks and Legal Protection of Personal Data Under the Technological Measures for Pandemic Prevention in Germany

Jui-Jen Pen*

Abstract

Since early March 2020, the daily number of confirmed COVID-19 infections has grown significantly in all states of Germany. To effectively curb the worsening pandemic, the German parliament quickly passed the "Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" and the "Das Zweite Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" in March and May respectively. It also approved the authorizations under the laws, which amended the provisions of the "Infektionsschutzgesetz" (IfSG). Articles 4 and 14 of the amended IfSG authorize the pandemic prevention agency "Robert Koch-Institut" (RKI) to develop an electronic reporting and information system that will be used to trace coronavirus infections and prevent its spread. The aforementioned "electronic reporting and information system"

* Deputy Director, Office of Science and Technology Policy, National Science and Technology Council; Adjunct Assistant Professor, Department of Political Science, Soochow University, Taiwan; Ph.D. in Economic and Social Sciences, University of Cologne, Germany.

is the Corona-App developed and promoted by the Bundesministerium für Gesundheit (BMG) and RKI.

After a user has voluntarily installed the app, it will locate his or her position and transmit contact data to a server of the government agency in charge of pandemic prevention for real-time tracking of the user's contact with any infected person within a certain distance and for the tracing of his or her movement. The transmitted data will be analyzed and used to quickly identify users who may have had contact with the infected person. They will be immediately recalled and isolated, and the next group of users possibly having had such contact will be identified. Even though the use of the app for pandemic prevention is legally permitted, its actual application has been controversial for the German academic circles in law and public health. When the app is running, all personal data collected by it is transmitted to the executive authorities for processing, regardless of whether such data is sensitive or ordinary. Therefore, it is inevitable that concerns arise over the infringement of personal and privacy rights due to misuse of personal data.

For opponents to the app, despite the voluntary nature of its use, it should not be hastily introduced because the law fails to specify the types, scope and methods of processing the personal data collected. For supporters of the app, however, excessive protection and overly conservative application of such data constitute a violation of the fundamental human rights in the "integrity of personal health". Both supporters and opponents of the app have their own arguments, but there is a lack of consensus. In this respect, this article will analyze the legality issues and subsequent controversies of human rights relating to the use of tracking apps and other technological means by the German government for pandemic prevention from the perspectives of the EU's "General Data Protection Regulation" (GDPR) and the domestic laws of Germany. The result of analysis will then be used for explanation of the solutions to the relevant legal controversies and serve as an important source of reference for the future research of laws on pandemic prevention.

Keywords: Infektionsschutzgesetz (IfSG), Corona-App, General Data Protection Regulation (GDPR), Protection of Sensitive Personal Data, Infection Tracing

1. 研究背景與問題意識

1.1 新冠病毒警示追蹤 App（Corona-Warn-App）的推動背景

自 2020 年 3 月初起，新冠肺炎（COVID-19）在歐洲多國快速擴散，包括德國在內，確診案例每日在各邦大幅增加。為有效減緩疫情惡化並控制感染範圍，德國自巴伐利亞邦（Bayern）起，聯邦及各邦政府均分別採取不同程度之限制公開場所出入，及隔離接觸者等相關措施。然而不論是聯邦或各邦，面對新型冠狀病毒（SARS-CoV-2）感染力超乎預期的緊急狀態下，皆依據德國國會於同年 3 月 27 日及 5 月 14 日快速通過立法之《全國範圍流行病情勢下之國民保護法》（Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite）及《全國範圍流行病情勢下之國民保護法第二次法案》（Das Zweite Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite）[1]，以及該法對《傳染病防治法》（Infektionsschutzgesetz, IfSG）、《國際健康規範執行法》（IGV-Durchführungsgesetzes）及《建築法》（Baugesetzbuchs）等相關法律條文修正後之授權，基於政府介入之必要性與不可替代性，快速制定限制部分基本人權（例如居住遷徙自由、秘密通訊自由及資訊自主權）之防疫措施[2]。

其中，在實體管制性防疫措施方面，包括邊境檢查、企業辦公室採遠距上班、各級學校停課、保持社交距離、搭乘大眾運輸工具配戴口罩等，另外

---

1 Bundesrat, Entwurf eines Zweiten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite, online verfügbar unter https://www.bundesrat.de/SharedDocs/drucksachen/2020/0201-0300/246-20.pdf?__blob=publicationFile&v=1 (zuletzt geprüft am Dez. 18, 2022).

2 Bianca Pettinger (Mai 14, 2020), Zweites Pandemiegesetz: Kein Datenschutz für Gesunde, Dr. Datenschutz, online verfügbar unter https://www.datenschutzbeauftragter-info.de/zweites-pandemiegesetz-kein-datenschutz-fuer-gesunde/ (zuletzt geprüft am Mai 17, 2020).

還有暫時限制行動自由的公共場所管制出入，以及除超市、藥局及特定機構或行業外，其餘商店暫停營業。再者，在科技工具追蹤措施方面，則包括「免疫護照」及快速增修後的《傳染病防治法》第 4 條及第 14 條[3]，授權防疫機構「羅伯特科赫研究所」及公共衛生主管機關，研發電子通報資訊系統，以投入感染源追蹤及擴散範圍掌控之用。而所謂之「電子通報資訊系統」即為德國聯邦衛生部（Bundesministerium für Gesundheit, BMG）及「羅伯特科赫研究所」開發並大力推動之「新冠病毒警示追蹤 App」（Corona-Warn-App，又稱 Tracing App，以下簡稱追蹤 App）[4]。

在大量民眾從平台下載安裝並同意使用後，透過個人定點及接觸資料回傳公共衛生主管機關之主機，及時並長期追蹤疑似感染者、確診者及與其接觸者之行動足跡，以達成控制感染範圍之防治目的。在追蹤 App 回傳資料分析比對後，可快速篩選出與確診者之可能接觸者，以及即刻召回、隔離及匡列下一波可能接觸者[5]，故可同時降低社會大眾在公共場所及企業員工在工作場域，因密集接觸而造成大量感染的風險。儘管已有法源依據，但追蹤 App 投入防疫的使用仍在德國法學及公衛學界產生爭議，特別是勞動相關法律尚無明確授權規定，允許企業雇主以保護員工健康為由，強制要求員工在公務或私人行動裝置安裝追蹤 App。因此，若企業雇主在未經過勞動契約協商下，即要求員工必須至少在公務用行動裝置安裝追蹤 App，則員工之工作權與隱私權保障如何兼顧，仍需加以釐清。此外，追蹤 App 技術本身雖已成熟，但應用時所蒐集之一般及敏感個資，均會被防疫機構儲存、處理及分析，故其中涉及人格權、隱私權、行動自由及個人資訊自決等基本人權，在防疫時期是否受到不當限制或侵害之疑慮，自有必要從歐盟與德國法制層面，進一步解析與探討。

---

3 §§ 4, 14 IfSG.

4 Bundesregierung, Corona Warn-App: Unterstützt uns im Kampf gegen Corona, Die Bundesregierung, online verfügbar unter https://www.bundesregierung.de/breg-de/themen/corona-warn-app (zuletzt geprüft am Aug. 9, 2020).

5 Bundesregierung (Fn. 4).

1.2 追蹤 App 是否採取強制安裝的兩難困境

關於追蹤 App 規劃、研發與推動的爭議，從 2020 年第二季疫情大幅擴散，且尚無疫苗時，就已開始。這當中針對追蹤 App 可能涉及個資與人權問題已有許多討論，但主要的討論爭點很少是針對是否應該開發追蹤 App，大部分仍在於如何設計一個有效的追蹤 App，以及是否強制民眾安裝使用[6]。但 2020 年初時的疫情在歐洲並不嚴重，所以防疫機構的焦點多放在國外，特別是來自中國或義大利的境外移入案例，對於本國因疫情擴散所需的防疫措施，尚在討論及初步施行階段。當時沒有人能預測，隨著義大利、西班牙等國疫情的加劇，歐洲大多數國家都紛紛陷入疫情中，因此德國聯邦與各邦政府分別頒布防疫措施，其中也包括保持社交距離及配戴口罩等。防疫機構「羅伯特科赫研究所」為此才真正著手研發追蹤 App，以落實社會距離的維持並減少不知情下的接觸傳染。追蹤 App 的出現來自於疫情大流行，但是否能減緩疫情尚不明確，就一般人而言，追蹤 App 不是大眾一開始就會選擇使用之科技工具，故反對者認為追蹤 App 的推出反而會誤導大眾對個資及隱私保護的觀念，若無法產生實際效果就該下架停用[7]。

反之，贊同開發追蹤 App 者認為，在有多種防疫措施及科技工具的前提下，並非追蹤 App 的使用率必須要超過 60%以上，才能發揮實際功用，因為到 2020 年 8 月為止，追蹤 App 的安裝比例雖不到德國人口總數之 20%，但感染趨勢短期內並未大量攀升或短期內大幅增加，所以追蹤 App 的應用效果仍不明確，但已漸漸浮現的正面效果。預期如果國民安裝使用的比例愈高，則透過距離偵測警示，減少接觸感染的成果也就愈好。對此，駭客組織「混沌電腦俱樂部」（Chaos Computer Club）雖不推薦民眾下載安裝，但對追蹤

6 Bundesregierung (Fn. 4).

7 Nicolas Kötter (Jun. 18, 2020), Die Corona-Warn-App – Fluch oder Segen?, Dr. Datenschutz, online verfügbar unter https://www.dr-datenschutz.de/die-corona-warn-app-fluch-oder-segen/ (zuletzt geprüft am Aug. 8, 2020).

App 功能與實際成效，卻未提出嚴厲批判[8]。

在追蹤 App 的程式研發與推動構想中，個人資料將在使用者依歐盟《一般資料保護規則》（General Data Protection Regulation, GDPR）第 4 條第一款及第 6 條第一項第一款 a[9]規定，於下載時經同意使用、儲存及處理。若追蹤 App 無法蒐集、處理個資，則其系統無法獲得可能感染者或確診者的資訊，亦無法及時提出警示。至於資料處理的範圍及公民個人權利可能受到影響的程度，並非僅是取決於個資使用的目的，而係必須有明確的法源依據[10]。聯邦政府決定新冠病毒 App 的使用，以及對個人資料的蒐集、處理，均須得到手機用戶的事前同意，以符合歐盟《一般資料保護規則》第 6 條第一項第一款 a 及第 7 條之規定[11]，而該追蹤 App 之營運及維護，則將交由防疫機構「羅伯特科赫研究所」。惟若追蹤 App 在實務上被當作特定公共場域、大眾運輸工具或其他公共服務的驗證和出入通行證之用，則追蹤 App 即非依自由意願使用，而有不得不使用之強制力。為了避免大量投入追蹤 App 可能對個人資訊自主權造成的危害，「聯邦資料保護專員」（Bundesdaten-schutzbeauftragte）及「資料保護協會議」（Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, DSK）應積極阻止追蹤 App 的直接強制使用[12]。

---

8 Marianne Westenthanner/Michael Humpa (Jul. 21, 2020), Die Corona App – Risiken und Nebenwirkungen, Chip 365, online verfügbar unter https://www.chip.de/news/Corona-Warn-App-So-sieht-sie-aus-das-kann-sie_182639402.html (zuletzt geprüft am Aug. 12, 2020).

9 Art. 4 Nr. 1 und Art. 6 Abs. 1 S. 1 Buchst. a DS-GVO.

10 Thomas Schwenke (Jun. 17, 2020), Corona-Warn-App als Pflicht für Mitarbeiter und Kunden (FAQ und Praxistipps)?, Datenschutz-Generator, online verfügbar unter https://datenschutz-generator.de/corona-warn-app-pflicht-nutzung/ (zuletzt geprüft am Aug. 10, 2020).

11 Art. 6 Abs. 1 S. 1 Buchst. a und Art. 7 DS-GVO.

12 Florian Rötzer (Mai 13, 2020), Datenerfassung von Gesunden: Lambrecht gegen Kelber, Heise Online, online verfügbar unter https://www.heise.de/tp/features/Datenerfassung-von-Gesunden-Lambrecht-gegen-Kelber-4719716.html (zuletzt geprüft am Mai 17, 2020);

但在間接造成的強迫使用方面，例如聯邦政府雖不能強迫人民都要使用追蹤 App，但若將追蹤 App 與個資連結後的警示功能，用於通行與否之驗證，則有違反《聯邦資料保護法》（Bundesdatenschutzgesetz, BDSG）及歐盟《一般資料保護規則》之虞，且民眾可透過一般司法程序加以救濟[13]。使用者依其自由意願安裝使用，雖未違反個資法規定，但追蹤 App 蒐集、處理及使用個資之範圍，並未詳細列舉規定於條文中。追蹤 App 於研發時的立法構想，原本並非採用自願安裝的推動方式，而是以立法強制民眾安裝使用，達成全面控制接觸確診者範圍的方式。如果採用特別法立法模式，則因相關法律要件可清楚列舉，故能減少許多法律不確定性帶來的爭議，以及對新法推動的阻礙。在立法過程中，資料保護法專家及聯邦眾議院綠黨黨團即有類似意見[14]。

但因聯邦政府最終未推動立法強制安裝追蹤 App，放棄以法律強制力要求民眾接受的作法，因此政府必須承認在無強制作用的情況下，宣導民眾安裝追蹤 App 的法不確定性，因為一旦追蹤 App 安裝受到條件限制，則須衡量追蹤 App 安裝比例如果偏低可能帶來防疫漏洞擴大的風險。然若為免除此等條件限制帶來政策措施推行的阻礙，則除於傳染病防治法中賦予公共衛生主管機關研發追蹤 App，另應課予一般民眾在無特殊原因等例外狀況下之安裝義務。但如果特別法中直接免除政府徵詢人民事先同意授權安裝，則追蹤 App 蒐集、儲存、處理或傳輸個資之功能，且未定義涉及使用個資的種類及範圍，則會牴觸《聯邦資料保護法》與歐盟《一般資料保護規則》[15]，不但追蹤 App 的使用無法律依據，不符法治國原則，且會因爭議過大而失去民眾

---

13 Schwenke (Fn. 10).

14 Schwenke (Fn. 10).

15 Schwenke (Fn. 10).

15 Rötzer (Fn. 12); Schwenke (Fn. 10); Connect.de, Zahlen-Schätzung zu Positiv-Fällen. Corona-Warn-App: So viele Infizierte haben sich gemeldet, online verfügbar unter https://www.connect.de/news/corona-warn-app-gemeldete-faelle-infizierte-positiv-zahlen-schaetzung-3200916.html (zuletzt geprüft am Aug. 5, 2020).

接受度，故最終聯邦政府並未採用修法課予強制安裝義務，仍維持符合現行法規定，以鼓勵方式促進民眾自願事先同意並授權系統後台使用其個資。但自願事先同意下載使用雖然可視為與合法性原則相符，但後續在行政機關的實際應用上，卻因為授權使用範圍不清，或過寬，而產生各界的爭論。

1.3　追蹤 App 之在個資使用層面形成之問題意識

新冠疫情防治已涵蓋公共衛生、流行病學，以及科技法律領域，其中更產生跨領域的議題與爭論。傳統醫療或公共衛生法律規範之探討，可能著重於生技醫藥研發、醫材製造品管、疫苗開發、人體實驗條件、疫調、公共衛生制度、防疫措施與紓困政策等。在臺灣，已有施行多年或快速通過之法制加以規範，例如《人體研究法》、《生技新藥產業發展條例》、《嚴重特殊傳染性肺炎防治及紓困振興特別條例》等。至於在數據與個資應用方面，臺灣則著重於遠距及智慧醫療，但此類科技之應用尚屬研發階段，抑或擬於立法中之醫療沙盒專法中進行實驗，因此並未針對不特定社會大眾進行大規模推廣，故對於 App 用於防疫工作進行個資蒐集等，臺灣除了《個人資料保護法》外，並無專法嚴格規定 App 等數位工具蒐集、儲存、傳輸及使用個資的要件。相對於歐盟及德國等國外法制，目前德國雖有蒐集及處理各類個資之相關法律規範，但在防疫期間仍無法完全排除個資被公共衛生主管官署、防疫機構、追蹤 App 上架平台或其他數位通訊傳輸服務商濫用的可能。法律雖賦予研發電子通報及資訊系統用於防疫之法源，然而相關法律規定之內容多著重於科技工具之運用方式與範圍[16]，但並無對敏感個資使用之具體規範。對此，本文將採用文獻分析法，透過蒐集、比對及深入分析德國聯邦政府官方出版品、法案文件、聯邦眾議院及參議院立法審議文件、民間團體諮詢意見、學者及專家見解，從法制層面以推行超過一年之「新冠病毒警示追蹤 App」為案例，於以下各節加以探討：

16 Bundesegierung, Corona-Warn-App. Die wichtigsten Fragen und Antworten, online verfügbar unter https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392 (zuletzt geprüft am Dez. 18, 2022).

1.在第 1 節與第 2 節中，除說明本文研究背景與主要問題意識外，將探討「新冠病毒警示追蹤 App」之系統運作模式，並從理論層次探討個資處理保護原則對追蹤 App 的檢視，以及歐盟《一般資料保護規則》（GDPR）與德國《聯邦資料保護法》（BDSG）等國內法，對追蹤 App 使用者之保護機制。

2.接著在第 3 節將就歐盟及德國法制，探討追蹤 App 於實際應用產生的爭議，其中包括「事前同意」在健康與資訊自主權間之歧異，還有從消費者保護之觀點討論「事先同意」可能的漏洞；AI 連結大數據對個人行為的側寫與追蹤 App 系統透明度不足之疑慮；追蹤 App 對「社會參與」的影響，以及其中正、反意見之論辯。

3.接續在第 4 節，將從勞雇契約關係及工作者保護之角度，分析追蹤 App 於工作場域的落實與推動條件，其中，包括雇主得要求員工安裝追蹤 App 之標準與個資使用原則對員工安裝義務的檢視，還有依據德國《聯邦資料保護法》規範判斷員工追蹤 App 安裝義務等。另外，追蹤 App 利用於公務與隱私領域間之區別，以及雇主對安裝於員工公務用手機之追蹤 App 發出警示時的通報義務等問題，亦會於本節中加以探討。

4.在本文第 5 節，將說明歐盟與德國追蹤 App 應用法制之後續走向，及防疫工作尚存之爭議，並提出本文之研究結論。

2. 追蹤 App 之運作模式與法律保護機制

2.1 「新冠病毒警示追蹤 App」（Corona-Warn-App）之運作原理及功能

為了有效降低接觸感染，或感染者未採檢前可能因不知情或不願遵守居家隔離檢疫，而四處流動，造成病毒散播幅度擴大的風險，除了限制行動等傳統緊急措施外，德國政府歷經三次緊急立法，並於第二緊急立法賦予防疫機構「羅伯特科赫研究所」開發「電子通報資訊系統」之權責，以促進民眾防疫之效能。所謂「電子通報資訊系統」係指近期完成上架之「新冠病毒警

示追蹤 App」（Corona-Warn-App），但在此之前，聯邦及各邦政府，還有醫療及資訊領域專家提出不同的科技防疫工具，例如行動電話細胞訊號定位即是其中之一。但科技工具在防疫的投入，不單是法律層面涉及敏感個資使用及限制人權之疑慮，連技術成熟與否的問題，也是重要的考量[17]。像是近來德國電信公司將匿名的行動電話資料轉送「羅伯特科赫研究所」，雖是為了控制疑似感染者接觸的範圍，但仍造成敏感個資外洩的疑慮。而此類傳送給防疫機構之敏感個資，除技術上須經過匿名處理外，且只能以集結後之數據型態進行追蹤，不能鎖定特定個人之行動足跡[18]。

先就行動電話定位來看，行動電話發出訊號之所在並非直接等同持有人所處之真正位置。電話基地台的細胞訊號資料，僅能提供特定行動電話與下一個基地台之間的大致距離。在大城市裡，透過基地台細胞訊號的衡量，定位之最高準確度可達 50 公尺範圍內，但是在鄉村地區，則細胞訊號與下一個基地台之間的測量則因距離遠近不一，而無法精準測量[19]。從技術層面可知，行動電話定位資料不能有效識別與確診者接觸之個人或群體，所以並不適用作為防疫之科技工具，除非是衛星定位，才有可能準確追蹤到數公尺的範圍內。但不論是行動電話或衛星定位，都必須經過用戶在 Android 及 iOS 作業系統上，自願打開並明確表示同意系統讀取 GPS 晶片之定位資料[20]。此種如同南韓、中國透過行動電話鎖定並分析其國內確診者個人行動之作法，已被德國聯邦資料保護專員否決，因此聯邦衛生部及防疫機構不得針對單一

17 BRAK, BRAK: Handyortung der Kontaktpersonen Corona-Infizierter nur als Ultima Ratio, online verfügbar unter https://rsw.beck.de/aktuell/daily/meldung/detail/brak-handyortung-der-kontaktpersonen-corona-infizierter-nur-als-ultima-ratio (zuletzt geprüft am Dez. 18, 2022).

18 Michael Rath/Gerrit Feuerherdt (Mär. 11, 2021), Corona-App, DSGVO und Co. Datenschutz in der COVID-19-Krise, Computerwoche, online verfügbar unter https://www.computerwoche.de/a/datenschutz-in-der-covid-19-krise,3548738 (zuletzt geprüft am Dez. 18, 2022).

19 BRAK (Fn. 17).

20 Rath/Feuerherdt (Fn. 18).

個人追蹤其足跡範圍。此種措施只有在緊急之特殊狀況且徵求廣泛之專業意見後，經由利害關係人同意下方得採用[21]。現階段在相關法律中，亦無直接授權聯邦衛生部或防疫機構，在未經當事人同意下，以「數位腳鐐」追蹤個人行動足跡之授權規定。所以行政機關並無直接法源依據可隨意追蹤個人行動，或相關辨識其行動範圍之位置資訊。另，也因行動電話資料可否被用於定位確診者足跡尚有法律爭議，且技術問題不易克服，故在最近兩波修法中，均未納入採用行動電話定位防疫之相關規定[22]。

除行動電話或衛星定位之外，使用科技工具防疫的方式還有採用「新冠病毒警示追蹤 App」，因為追蹤 App 需透過 Google 或 Apple 的平台下載，所以必須得到用戶明確的自願同意才能安裝，其對個資的使用屬於合法範圍。追蹤 App 會使用行動電話或行動裝置內建的藍芽功能，在最小的效力範圍內，透過傳輸、使用最小化之個資，取得接觸確診者資訊，以藉此判斷哪些疑似感染者、確診者或隔離者目前與行動電話使用者處於近距離的範圍[23]。當用戶啟動 App 後，行動裝置內之系統透過藍芽偵測固定距離，並會隨機產生一組匿名、加密並儲存於各個行動裝置中的臨時識別身分。如果接近行動電話用戶者是新冠肺炎確診者，則儲存於行動裝置中的識別身分會透過追蹤 App 向中央伺服器發出訊號，並於行動裝置偵測之適當距離在特定時間內並未改變（例如已遠離原位置）的情況下，中央伺服器會向接近之兩人的行動裝置發送警示訊息，並同時要求接觸疑似感染者或確診者之用戶立即

21 Brink, Stefan und Clarissa Henning (Apr. 3, 2020), Digitalisierung in der Corona-Falle: Warum freiwilliges Handy-Tracking nicht funktioniert, Netzpolitik.org, online verfügbar unter https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert/ (zuletzt geprüft am Dez. 18, 2022).

22 Rath/Feuerherdt (Fn. 18).

23 Christian Stör (Mär. 31, 2020), Corona-Virenschutz: Handy-Daten nutzen oder nicht - ist die App die Lösung?, Frankfurter Rundschau, online verfügbar unter https://www.fr.de/meinung/corona-virenschutz-handy-daten-nutzen-app-loesung-13634597.html (zuletzt geprüft am Mai 20, 2020); Rath/Feuerherdt (Fn. 18).

與他人隔離，用以減少接觸感染及病毒擴散的風險[24]。依照追蹤 App 原先之設計，行動裝置訊號與中央伺服器之間的傳輸與處理過程均為匿名，且測試程序是在自有的行動電話或裝置中執行，不會洩漏識別用戶個人真實身分之個資或其所在之位置資訊。由於追蹤 App 必須是由民眾自願下載及安裝，所以社會大眾的疑慮減少，在防疫階段的接受度逐漸增高[25]。

「羅伯特科赫研究所」委託民間業者開發的追蹤 App 在不斷補充功能下，目前已經到 2.3 版，且具有接觸狀況紀錄、PCR 檢測結果紀錄、數位疫苗接種護照（綠色護照）等數位功能，但因此類功能涉及聯邦政府或各邦政府依法制定與執行之防疫措施、疫苗接種計畫和疫情趨勢分析等權責，所以必須由法定傳染病防治機構「羅伯特科赫研究所」處理相關醫療個資或確診者資訊。而且「羅伯特科赫研究所」為唯一法定得公告重大疫情資訊及建議政府防疫方式之機構，故 App 蒐集的資料會傳輸至「羅伯特科赫研究所」進行比對，並用於避免個人接觸及群聚感染之分析。至於 Apple 或 Google 等數位平台在德國並無自行開發之警示追蹤 App，此等平台只提供 App 上架陳列、通知、說明與下載服務等通路功能。同時，數位平台並非防疫主管官署，若自行研發 App 可能涉及醫療特種個資使用爭議，雖仍可以自願同意下載使用適用阻卻違反要件，但不符其平台經濟效益，公信力可能亦低於「羅伯特科赫研究所」，故 Apple 或 Google 等平台多採配合推動追蹤 App 的態度，但不自行開發[26]。

2.2 「羅伯特科赫研究所」接收行動裝置訊號後之處理

追蹤 App 能運作的關鍵除了兩大平台業者的作業系統外，還有就是用戶同意安裝後，透過行動電話或裝置開啟追蹤 App 後蒐集與傳輸至「羅伯特科

24 Rath/Feuerherdt (Fn. 18).

25 Stör (Fn. 23).

26 Infektionsketten digital unterbrechen mit der Corona-Warn-App, Robert Koch Institut, online verfügbar unter https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (zuletzt geprüft am Dez. 18. 2022).

赫研究所」進行即時處理的用戶行動資料，其中也包括個人 IP 位置定位後之行動足跡與範圍等地理資訊，以及使用者個人最新之採檢結果，又因後台系統會比對確診者之敏感醫療資訊，所以又會使用到特種個資[27]。若按照「羅伯特科赫研究所」的說明，追蹤 App 技術上的確會短暫使用到用戶的個資，但是在接受到用戶端 IP 位置資訊並於比對回覆後，系統將會直接刪除中央伺服器內的用戶位置資訊、個資及比對結果（是否與確診者近距離接觸）。從技術之理論層面而言，「羅伯特科赫研究所」的中央伺服器，確實會有短暫時間儲存並處理收到的個資，但系統在刪除前是否有另外傳輸他處或做其他分析之用，則未有明確之說明[28]。

另依「羅伯特科赫研究所」的使用說明可知，其開發的追蹤 App 透過系統蒐集的個資超過 14 日之後，即會自動刪除，不會再儲存於資料庫中。以 14 日為儲存期限的依據在於，經過藍芽系統偵測產生的訊號不會直接回傳個人姓名，而是以隨時產生的代號，以匿名化的格式回傳主機後儲存，所以理論上防疫主管官署，例如德國聯邦衛生部，應無法直接從儲存於資料庫中的個別資料，識別被回傳者之真正身分[29]。就歐盟《一般資料保護規則》及德國《聯邦資料保護法》規定而言，僅有依據蒐集目的的儲存要件，但並無儲存期限之規定。舉例來說，在勞雇關係存續中，雇主得與勞工在勞動契約中約定個資儲存期限，或依法定期限保存個資，像是所得稅相關資料等需保存 7 年，但通常在勞雇關係消滅後，雇主就不得繼續保留離職員工之個資，必須加以刪除，否則即違反蒐集目的[30]。

---

27 Bundesegierung (Fn. 16).

28 Kötter (Fn. 7).

29 Bundesegierung (Fn. 16).

30 Patrick Majcen (Apr. 26, 2018), Praxishilfe Datenschutz: Wie lange darf ich personenbezogene Daten speichern?, Ikonline, online verfügbar unter https://www.lko.at/praxishilfe-datenschutz-wie-lange-darf-ich-personenbezogene-daten-speichern+2400+2704442 (zuletzt geprüft am Okt. 19, 2021).

2.3　追蹤 App 涉及之個資保護原則[31]

作為法定「電子通報資訊系統」之「新冠病毒警示追蹤 App」利用藍芽設備測量社交距離範圍內可能之接觸者[32]，比直接定位行動電話細胞訊號範圍追蹤接觸確診者更為準確，且以該用戶為中心匡列周遭可能接觸者，並以每一個被匡列之接觸者為基準，進一步擴大追蹤更多之接觸者或未依規定隔離之確診者[33]。科技工具的應用確能迅速防治病毒傳染範圍，然而採檢結果不論是否感染均為具機敏性之醫療資訊，應屬歐盟《一般資料保護規則》第 9 條規定之敏感（特種）個資。雖然追蹤 App 必須經由用戶本人事先同意後，才能下載安裝，但追蹤 App 的後台系統畢竟會蒐集與傳輸個資，尤其是確診與否的特種個資，即使是經過同意仍需符合前述歐盟《一般資料保護規則》規範之個資處理原則[34]，儘量減少「事先同意」可能導致防疫主管官署採行之「措施」（使用追蹤 App 追蹤確診足跡），與「目的」（為阻擋病毒擴散而使用個資）間不合比例原則的狀況，以及防疫主管機關透過追蹤 App 系統連結資料庫，不當擴張使用範圍，或違反既有蒐集個資目的，並用於他處（例如用於醫療研究）的濫用行為。

關於個人資料處理應依循的基本原則，規定於歐盟《一般資料保護規則》第 5 條第一項[35]各款，其中涉及追蹤 App 使用個資者，包括「處理之合

31 Madeleine Kümmerle (Mär. 3, 2022), Wichtige Datenschutzgrundsätze für die Verarbeitung von Daten, Dr. Datenschutz, online verfügbar unter https://www.dr-datenschutz.de/dsgvo-grundsaetze-fuer-die-verarbeitung-personenbezogener-daten/ (zuletzt geprüft am Dez. 18, 2022).

32 Maike Weiss/Kathrin Strauß (Apr. 6, 2020), Corona und Datenschutz: Wie Handyortung im Kampf gegen das Virus helfen soll, Datenschutzexperte.de, online verfügbar unter https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/corona-und-datenschutz-wie-handyortung-im-kampf-gegen-das-virus-helfen-soll/ (zuletzt geprüft am Mai 17, 2020).

33 Rath/Feuerherdt (Fn. 18).

34 Kümmerle (Fn. 31).

35 Art. 5 Abs. 1 DS-GVO.

法性」（Rechtmäßigkeit der Verarbeitung）[36]、「依忠實與信賴處理」（Verarbeitung nach Treu und Glauben）[37]、「透明度」（Transparenz）[38]、「目的性連結」（Zweckbindung）[39]、「資料使用最小化」（Datenminimierung）[40]、「資料處理正確性」（Richtigkeit der Datenverarbeitung）[41]、「儲存限制」（Speicherbegrenzung）[42]、「完整與保密」（Integrität und Vertraulichkeit）[43]等，例如特種個資的使用，必須符合事先同意下載追蹤 App 時，最初授權蒐集、儲存及使用個資之目的，亦即不能違反「目的性連結」。同時，同意使用個資之範圍亦須依「資料使用最小化」原則，只擷取最必要之部分，例如只使用身分證號碼及電話就足以識別，那就避免使用姓名、生日、職業、地址等個資，降低不必要使用之程度。與此相關者，則是「儲存限制」，意思是儲存於系統後台的個資，應儘量以「假名化」（Pseudonymisierung）之儲存格式進行去識別化，以減少個資被回推識別的機率，而個資在儲存及使用目的不存在時，即應加以刪除。另在「資料處理正確性」及「完整與保密」原則方面，追蹤 App 個資處理過程中，應建置適當之科技保護措施，以免個資於處理中外洩，或遭到他人未經授權的使用或濫用。此一安全措施亦須保護個資的完整，避免因負責人員處理不當，或因其他外力而毀損、遺失[44]。

除了上述歐盟《一般資料保護規則》第 5 條第一項規定之原則外，依德國《傳染病防治法》（IfSG）第 14 條亦有應目的性原則與透明化原則之共同

---

36 Art. 6 Abs. 1 DS-GVO.
37 Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 Buchst. a i. V. m. und Art. 7 DS-GVO.
38 Art. 5 Abs. 1 Buchst. a, Art. 12, Art. 25 und Art. 42 DS-GVO.
39 Art. 5 Abs. 1 Buchst. b DS-GVO.
40 Art. 5 Abs. 1 Buchst. a DS-GVO und § 3 BDSG.
41 Art. 5 Abs. 1 Buchst. a und Art. 17 Abs. 1 Buchst. d DS-GVO.
42 Art. 5 Abs. 1 Buchst. e 2. Hs. und Art. 17 Abs. 1 Buchst. a DS-GVO.
43 Art. 5 Abs. 1 Buchst. f und Art. 32 DS-GVO.
44 Weiss/Strauß (Fn. 32); Kümmerle (Fn. 31).

規定，追蹤 App 實際投入個人行動訊息追蹤，應具備以下要件[45]：

1.安裝及使用追蹤 App 應取得用戶自願事前同意授權，並在用戶檢查及管理下執行。因此在未徵詢用戶再次同意，或依法律規定，個資之使用只限於最近一次之授權條款所揭示之範圍，逾越授權範圍轉為他用或二次利用係屬禁止行為。

2.追蹤 App 相關功能之執行必須維持最高比例之透明度。用戶應被告知，有哪些具特定功能的程式被載入，且安裝後，哪些程式功能會蒐集哪些個人資料，蒐集之範圍是否為必要程度，且這些資料被誰用於何種目的。其中，也應包括非目的性轉用之禁止，還有資料保存地點。

3.特種或一般個資應於用戶所在地點蒐集並直接在地儲存及處理，並只有主管機關或經法律授權之防疫機構（例如羅伯特科赫研究所）得為防疫目的使用、分析及確認接觸者資料。

4.所有的資料應儘量以匿名化處理，而個人識別資料至少要用假名化或無法識別之代號替代真實姓名。

5.公共衛生主管機關及防疫機構不得無故擷取或轉存追蹤 App 蒐集之特種或一般個資，所有個資僅於特定期間內儲存或處理，逾期者應以無法回復之方式銷毀[46]。

2.4 「事先同意」作為個資例外使用之論述

在疫情擴散期間，為了有效防治新冠病毒擴散，並漸少接觸感染，數位科技的運用，特別是追蹤 App 的研發與使用，已成為重要的討論議題，其中更關係現行法的法律調適或增修。特別是追蹤 App 的功能涉及個人資料的傳

45 Peter Schaar (Mär. 30, 2020), Peter Schaar: Mit heißer Nadel gegen das Virus?, Heise Online, online verfügbar unter https://www.heise.de/newsticker/meldung/Peter-Schaar-Mit-heisser-Nadel-gegen-das-Virus-4693535.html (zuletzt geprüft am Mai 17, 2020).

46 Friedhelm Greis (Mai 28, 2020), FAQ zur Corona-App der Bundesregierung, Golem.de, online verfügbar unter https://www.golem.de/news/faq-was-man-ueber-corona-app-der-regierung-wissen-muss-2005-148749.html (zuletzt geprüft am Jun. 1, 2020).

輸、儲存與處理，所以如何保護個資，更是法學界對於防疫與人權衝突該如何平衡的爭論焦點[47]，而個人「事先同意」作為阻卻違法要件之法源依據及爭議，一直是重要的討論焦點。其中，追蹤 App 運作中所使用之匿名資料，並非大多數人所認知之歐盟《一般資料保護規則》的規定範圍[48]，從個人資料定義的反面推論及歐盟《一般資料保護規則》第 26 點衡量理由[49]中可知，匿名資料必不屬於歐盟《一般資料保護規則》效力所及之範圍，因此傳輸、儲存及使用匿名化資料的追蹤 App，將不受個人資料保護法規之限制，因為不論是歐盟《一般資料保護規則》，還是德國《聯邦資料保護法》，都未以相關條文規定，此等無法立即識別身分的匿名資料如何使用，抑或使用之要件[50]。

早在歐盟《ePrivacy 指令》（Datenschutzrichtlinie für elektronische Kommunikation）第 5 條[51]關於資料儲存於用戶終端設備，需徵求事先同意之規定，又再次引起外界之討論，因為受到疫情持續惡化，疫苗施打的普及率仍然偏低，因此追蹤 App 難以判定成效，讓個人資料的絕對保護是否必要藉由「事先同意」而排除，出現了質疑及爭議。其中，學界從個人資料保護法制的角度認為，追蹤 App 在防疫的投入應是選項之一，因此可考慮其能產生的效果，但不能視為必須出現防疫的作用，以致於下載、安裝被當作一種義務，即使仍須通過事先同意，惟一旦追蹤 App 的使用被視為一種標準或門檻，則事先同意的要件，並不能確認個人是基於自願而同意授權[52]。歐盟

47 Darko Samardzic/Thomas Becker, Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW 2020, S. 646 (648).

48 BNetzA (2020), Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, Bundesnetzagentur, online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile (zuletzt geprüft am Apr. 3, 2021).

49 Erwägungsgrund 26 der DS-GVO.

50 Samardzic/Becker (Fn. 47), S. 648.

51 Art. 5 der Datenschutzrichtlinie für elektronische Kommunikation.

52 Samardzic/Becker (Fn. 47), S. 649.

《一般資料保護規則》雖有對個人資料保護嚴格的規定，但受到規範者，限於處理個人資料的公共衛生官署或防疫機構，但追蹤 App 系統本身，並未受限於歐盟《一般資料保護規則》的規定。儘管在疫情壓力下，任何會使用個人資料的數位工具如追蹤 App 等，都無法免除授權範圍的檢視，特別是在歐盟《一般資料保護規則》的法律架構下，追蹤 App 雖可基於個人自願的事先同意而使用個人資料，但所謂「自願」和「事先同意」之範圍、種類、時限、使用條件、利害相關人資料保護，以及在法治國原則下的意涵等，仍待進一步的釐清與檢視[53]。

2.4.1 「自願」及「事先同意」及法治國原則之必要性

目前追蹤 App 的倡導及推動，都必須依據「自願」（Freiwilligkeit）同意原則，而此「自願」的法理概念，也被視為與歐盟《一般資料保護規則》第 6 條第一項第 a 款及第 7 條[54]中所規定之「個人資料處理事先同意授權」相符，儘管「自願」只是歐盟《一般資料保護規則》第 4 條第一項第十一款[55]規定事先同意的條件之一，但已可被視為一項符合「法治國原則」中之「必要性」（Erforderlichkeit）的替代要件。

「自願」及「事先同意」是同時被視為建構個人資料保護機制的基本元素，「事先同意」被歐盟《一般資料保護規則》第 6 條第一項[56]當作個人資料處理之阻卻違法要件，而此一要件是實際上，專為允許個人資料處理之獨立阻卻違法要件，其中針對「事先同意」共有六項明確之基本構成要件[57]。重要的是，「自願」及「事先同意」同屬重要的資料保護權概念下的原則，故而用戶以其主觀意志決定個人資料是否交由第三人使用的權利，係屬於

53 Samardzic/Becker (Fn. 47), S. 649.

54 Art. 6 Abs. 1 S. 1 Buchst. a und Art. 7 DS-GVO.

55 Art. 4 Abs. 1 Nr. 11 DS-GVO; Achim Klabunde, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, § 4 Rn. 20.

56 Art. 6 Abs. 1 DS-GVO.

57 Benedikt Buchner/Thomas Petri, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG Kommentar, 2. Aufl., 2018, § 6 Rn. 1 ff.; Samardzic/Becker (Fn. 47), S. 649.

《德國基本法》第 1 條第一項及第 2 條第一項[58]規定推演出的個人「資訊自主權」（informationelle Selbstbestimmung），及此一權利的具體展現[59]。除此之外，個人資料應受保障的原則，亦源自於個人人格權及人類尊嚴的基本人權要求。在歐盟現代人權的分類中，資料保護是作為一種獨立、個別之基本權利，尤其是《歐盟憲章》（Charta der Grundrechte der Europäischen Union）第 8 條第一項及《歐盟運作條約》（Vertrag über die Arbeitsweise der Europäischen Union, AEUV）第 16 條第一項[60]中的規定，是具高度優先性之重要基本規範[61]。

2.4.2 個人資訊自主權之「抵抗權」與「固有本質論」

「資訊自主權」作為個人資料保護必要性之核心原則，具有兩項之主要理論依據。其一為個人「抵抗權」之論點，如果個人不同意相關被傳輸資訊中含有涉及個人背景的內容，則應有權利抵抗、反對此類資訊的外洩、散播或被利用[62]。其二則為「固有本質論」，意即個人一方面有權自行決定訊息的內容及揭露的範圍，另一方面也可自行決定，是否允許他人在特定個人相關資訊範圍內，蒐集及處理具有個人資料的資訊。而個人對資訊內容及使用的自主決定權，是不得受到任何的限制。在《歐盟憲章》第 8 條第二項[63]即有很明確的規定，「事先同意」是個人資料處理的法律依據[64]。在一般人的

58 Art. 2 Abs. 1 i.V.m. und Art. 1 Abs.1 GG.

59 BVerfGE 150, 244; NJW 2019, 827; BVerfGE 65, 1; NJW 1984, 419; René Firgt, Strukturelle Analyse des allgemeinen Persönlichkeitsrechts anhand des Rechts auf informationelle Selbstbestimmung, 2015, S. 128-130.

60 Art. 8 Abs. 1 EU-Grundrechtscharta mit Art. 16 Abs. 1 AEUV.

61 Samardzic/Becker (Fn. 47), S. 649; Heinrich Amadeus Wolff, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar zu EUV, GRC und AEUV, Bd. II, 2017, § 8 Rn. 1 ff.

62 Art. 8 Abs. 2 S. 1 EU-Grundrechtscharta; Michael Friedewald/Jörn Lamla/Alexander Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 63-64; Samardzic/Becker (Fn. 47), S. 649.

63 Art. 8 Abs. 2 EU-Grundrechtscharta.

64 Sibylle Gierschmann/Katharina Schlender/Rainer Stentzel/Winfried Veil, in: Gierschmann

各種生活領域中，只要涉及隱私，都會與個人資訊自主權有關，因此個人能否依其自我意志決定資訊的內容與使用的方式，屬於應被保障的基本人權之一。經由個人自由意志決定對外表示的同意授權，將成為全面性的阻卻違法要件。

只要有個人對外表述的同意授權他人進行資料處理，則後續對於此人的個人資料處理及使用，就會具有法律依據，而在個人提出其「事先同意」時，並不需要滿足任何條件，也不需要以法律衡量或規範的檢視，賦予事先同意阻卻他人進行資料處理的違法性[65]。雖然在歐盟《一般資料保護規則》第 6 條第一項第 b 款至第 f 款[66]規定之阻卻違法要件中，都有明文「必要性」（erforderlich），但是在第 6 條第一項第 a 款[67]，則以「事先同意」作為阻卻違法的唯一要件，並不需要檢視其「必要性」[68]。另，歐盟《一般資料保護規則》第 7 條第一項至第四項[69]規定須取得「事先同意」，除了有權處理個人資料者須提出相關人之事先同意、提出事先同意之形式與方式，以及個人意志之自願、隨時可撤回同意授權等，資料處理相關人之條件外，並無將「必要性」作為同意門檻之規定。在歐盟《一般資料保護規則》第 6 條及第 7 條[70]規定的立法理由，係根據憲法層級的保障規範（例如《歐洲人權公約》、《歐盟憲章》及《德國基本法》等），其背後之立論在於任何人都有權利依其自由意志，經過深思熟慮之後，在未受強迫下，探詢所需訊息或挑選有用資訊[71]。對此，任何人依法都不應遭受不公平、不合理或歧視的對待。而此一立論及其背後保障人權的假設，也成為歐盟《一般資料保護規

(Hrsg.), Kommentar DS-GVO, 2018, § 6 Rn. 47.

65 Gierschmann/Schlender/Stentzel/Veil (Fn. 64), § 6 Rn. 48.

66 Art. 6 Abs. 1 Buchst. b bis f DS-GVO.

67 Art. 6 Abs. 1 Buchst. a bis f DS-GVO.

68 Buchner/Petri (Fn. 57), Rn. 15; Samardzic/Becker (Fn. 47), S. 649.

69 Art. 7 Abs. 1 bis 4 DS-GVO.

70 Art. 6 und 7 DS-GVO.

71 Samardzic/Becker (Fn. 47), S. 649.

則》保障之個人資訊自主權下，各類阻卻違法要件的重要建構基礎。對於追蹤 App 的提供平台與公共衛生官署而言，在人人都有資訊自主權的前提下，經由自願提供之事先同意授權，無疑是開啟追蹤 App 在防疫期間蒐集、傳輸、儲存及處理個人資料之最大與最寬鬆的裁量範圍。這也表示，不論個人資料受到如何嚴格的管制，但只要符合事先徵詢同意授權的簡單條件，則再嚴格的管制也能即刻鬆綁，降於最低限度[72]。

2.5 透過「事前同意」落實之合法性原則與現行法規定

歐盟《一般資料保護規則》的立法者認為，因國家機關與人民之間呈現一種上下從屬的關係，人民並不知道國家機關如何利用他們的個資，因此相對於國家機關，法律應賦予人民要求事先同意之權利，而作為行政機關之防疫主管官署，應依法徵求人民事先同意授權，才能以追蹤 App 的後台系統使用個資，此即歐盟立法者強調之「處理之合法性」（Rechtmäßigkeit der Verarbeitung）原則。這表示，追蹤 App 任何以防疫目的對個資的蒐集與處理，都必須有法律依據。在歐盟《一般資料保護規則》第 42 點立法衡量理由[73]中曾表示，當利害關係人個人有自由或真正之選擇權利，且處於有行使此一能力的狀態時，得依其自由意願授權第三人使用其個資、拒絕授權第三人使用其個資，或撤回其授權，且不受任何歧視或不當對待[74]。接著在歐盟《一般資料保護規則》第 43 點立法衡量理由[75]也有相關之闡述，「為確保同意授權是自願為之，當利害關係人（或當事人）與具權責者間明顯處於不對等之關係，特別是具權責者為行政官署或與官署有關，且又經考量所有狀況後，即使是在特有例外下，利害關係人都不可能會自願授權具權責之人使用其個資，則該具主管權責者（或官署）無使用此人個資之法律依據。」[76]

72 Samardzic/Becker (Fn. 47), S. 649.
73 Erwägungsgrund 42 S. 4 DS-GVO.
74 Kötter (Fn. 7).
75 Erwägungsgrund 43 DS-GVO.
76 Kötter (Fn. 7).

在國內法層次之法源依據，德國《聯邦資料保護法》第 26 條第三項第二款[77]也再次強調，同條第二項對於一般個資處理須經由事先同意之要件，同樣適用於特種個資之處理，而且相關人事先授權並須與所被處理個資之間，具有明確及詳細的關聯；同條第三項第三款[78]則規定，在《聯邦資料保護法》第 22 條第二項[79]納入之個資處理應採取適當措施，以防止或降低利害關係人自由、權利受侵害風險之規定，亦適用於勞資關係存續中，因必要而進行個資處理之狀況。追蹤 App 傳輸後的資料或被處理後的資料，都需儲存於具安全防護機制之設備，但儲存之個資依其性質與內容，可能與公共利益有關，在已無符合蒐集目的之狀況下，必須加以刪除或直接銷毀。然而，大量儲存的個資可能涉及公共利益，例如群體免疫數據、流行病感染與傳播趨勢等，關係日後改善公共衛生與擬定傳染病防疫政策，故此類資料有長久建檔保存之必要。對此，《聯邦資料保護法》第 28 條第一項[80]亦規定，基於公眾利益之資料建檔保存必要者，亦得處理歐盟《一般資料保護規則》第 9 條第一項[81]所定義之特種個資，但負責人員必須採取符合《聯邦資料保護法》第 22 條第二項第二款[82]所規定之標準，適當且具實際保護作用之技術措施，以保障個資相關人權益，不致因建檔保存而受到損害。

追蹤 App 雖為免費下載、安裝及使用，但數位平台提供上架服務時必然也有相對應之定型化契約條款，仍需經由個人事先同意，因此使用者於下載安裝時，必然已同時同意 App 本身之使用條款，與數位平台提供下載服務之契約條件。因此平台與使用者間，因定型化契約的同意、解除或後續爭議，而涉及《聯邦資料保護法》第 31 條[83]對信用評分查詢在商業交易過程之保護

77 § 26 Abs. 3 S. 2 BDSG.
78 § 26 Abs. 3 S. 3 BDSG.
79 § 22 Abs. 2 BDSG.
80 § 28 Abs. 1 BDSG.
81 Art. 9 Abs. 1 DS-GVO.
82 § 22 Abs. 2 S. 2 BDSG.
83 § 31 BDSG.

（Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften）。在符合《聯邦資料保護法》第 31 條第一項第一款至第四款[84]要件之前提下，為決定與相關人（自然人）之契約締結、履行或結束，得使用預測此一契約相關人未來特定行為模式，所做出之概率值[85]，然而經由數位函式或統計模型產生之估計結果，涉及個人隱私及資訊自主權，故必須符合第 31 條第一項各款列舉符合個資保護之法律要件，其中，用於計算概率值之資料，必須是在科學承認之統計計算下，用於證明特定行為發生概率之估計結果相當顯著。再者，用於計算概率值所使用資料，不能只有通訊地址，而計算程序若需使用個人通訊地址，則在估計行為模式概率前，必須先告知個資相關人，並加以記錄。

至於在告知義務方面，歐盟《一般資料保護規則》第 13 條第三項[86]規定，若負責人員欲將個資用於其他目的，則負責人員於進行個資處理前，應先告知當事人其變更後之使用目的。同時，還須依據歐盟《一般資料保護規則》第 13 條第二項[87]各款規定，向相關人說明資料儲存時間、當事人詢問個資權利、要求刪除或限制個資處理，以及撤回個資處理或轉移之授權等重要資訊。對此，德國立法者在《聯邦資料保護法》第 32 條中[88]，針對歐盟《一般資料保護規則》第 13 條第三項[89]負責人員於原蒐集目的外使用當事人個資之徵詢義務，及第 13 條第四項[90]之例外規定，另又補充更詳細之免責要件。由此可知，《聯邦資料保護法》第 32 條[91]在與歐盟法一致的前提下，雖要求負責人員處理個資與原蒐集目的不一致時，應履行通知義務，但仍增加更多國內法層級的阻卻違法要件。例如歐盟《一般資料保護規則》第 23 條第一項

84 § 31 Abs. 1 S. 1 bis S. 4 BDSG.

85 此處係指統計模型產生之估計值，或依據公式估算出之結果。

86 Art. 13 Abs. 3 DS-GVO.

87 Art. 13 Abs. 2 DS-GVO.

88 § 32 BDSG.

89 Art. 13 Abs. 3 DS-GVO.

90 Art. 13 Abs. 4 DS-GVO.

91 § 32 BDSG.

第 a 款至第 j 款[92]即規定，經由負責人員或受委託處理者依循之歐盟法或成員國法律條文，若與歐盟《一般資料保護規則》第 12 條至第 22 條[93]所列舉之權利義務不一致，則依歐盟《一般資料保護規則》第 12 條至第 22 條、第 5 條、第 34 條[94]規定，得經由各該成員國國會以立法程序加以限制。

惟此等限制必須尊重人權與個人自由之基本原則，具有符合民主運作與法治國原則考量之必要性，且另有採取符合比例原則之保護措施，用以確保國安、國防與公共安全，或用於預防、調查、揭露及追蹤刑事犯罪，以及執行刑罰、保護民眾免受犯罪危害並防備危險發生等。其次，前述以國內法規定阻卻違法要件之目的，還包括保護其他更重要之歐盟或成員國公共利益，特別是歐盟或成員國重要之經濟或金融利益，例如貨幣、預算、稅務，以及公共衛生與社會安全，還有司法獨立、法院程序之保護等。另外，因違反歐盟《一般資料保護規則》第 23 條第一項第 a 款至第 e 款[95]規定而被監控之職業所涉及之預防、揭露、調查及追蹤工作，以及為維護公權力特在定期間限制、檢查、監控及維持秩序之功能，還有相關人或其他人權利與自由之保護和民事請求權之執行等，均適用上述以國內法規定阻卻違法之規定。

目前歐洲各國具有防疫權責者，多為行政機關。在德國，防疫政策制定為主管公共衛生事務之聯邦衛生部，而直接執行防疫相關措施者為「羅伯特科赫研究所」。該機構之性質在追蹤 App 研發時所作資料保護風險評估中，即被認為是具有國家機關性質，亦為執行防疫之權責機關[96]。但不論是聯邦衛生部，抑或身為第一線防疫機構的「羅伯特科赫研究所」，為了防疫而使用科技工具蒐集、儲存、處理及使用個資，自不能免除徵詢個人之自願同意

92 Art. 23 Abs. 1 Buchst. a bis j DS-GVO.

93 Art. 12 bis 22 DS-GVO.

94 Art. 12 bis 22, Art. 5 und Art. 34 DS-GVO.

95 Art. 23 Abs. 1 Buchst. a bis e DS-GVO.

96 Datenschutz-Folgenabschätzung (DSFA) für eine Corona-App, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), online verfügbar unter https://www.fiff.de/presse/dsfa-corona-digiges.html (zuletzt geprüft am Aug. 10, 2020).

授權，而且追蹤 App 經由用戶同意授權的範圍，包括「羅伯特科赫研究所」及防疫主管機關在內，亦不得依行政措施臨時需要，任意變更範圍，亦不能於未經過再次徵詢或依歐盟或其他國內法規定，違反蒐集目的轉於其他公共衛生或醫療研究用途。相對地，「羅伯特科赫研究所」雖主導防疫，但畢竟不是一般行政機關，所以並無直接裁量給付行政之法定權力，即使民眾不同意授權使用個資或拒絕安裝 App，也不能拒絕人民依法提出之服務提供要求[97]。「羅伯特科赫研究所」接受政府委託開發的追蹤 App，不但不能由該機構直接作為執行防疫政策的強制工具，而要求人民使用，亦不得將安裝 App 設定為行政機關提供各類公共服務或社會福利的准駁依據[98]，藉此免除徵詢事前同意授權的義務。

2.6 「自願」及「事前同意」在個資使用上之意涵與論辯

追蹤 App 的使用，需要取得用戶（或其他利害關係人）的事前同意（Einwilligung）後，才能安裝並啟動功能，而「事前同意」的要求，也符合歐盟《一般資料保護規則》第 6 條第一項第 b 款[99]的規定，作為蒐集及處理個人資料的阻卻違法要件[100]。就德國法而言，在實務上的討論，為能在必要時解除限制，故有很多法律是依據「自願」（Freiwilligkeit）原則，作為重要的法源。但「自願」與用戶之「事前同意」，在概念上雖不完全相同，在實務上很難從客觀的標準加以區分。所謂的客觀合法的保護，既然係以「事前同意」為要件，所以很難從中再去推導出其他同樣可適用的例外，自然也難以被利害關係人的個人「自願」所替代[101]。但目前生效中的歐盟《一般資料保護規則》及德國《聯邦資料保護法》，對於個人資料在客觀法律要件上的

97 FIfF (Fn. 96); Kötter (Fn. 7).

98 Kötter (Fn. 7).

99 Art. 6 Abs. 1 Buchst. a DS-GVO.

100 Sebastian Schulz, in: Gola (Hrsg.), Datenschutz-Grundverordnung (DS-GVO) Kommentar, 2. Aufl., 2018, § 6 Rn. 21 ff.

101 Samardzic/Becker (Fn. 47), S. 648.

保護，卻因個人事前同意的主觀授權，而失去其原本嚴格限制的作用[102]。

儘管如此，仍不能認為歐盟《一般資料保護規則》及德國《聯邦資料保護法》是自我解除規範的效力，因為個人的事前同意，仍係相關人自我意志所表達的同意授權，因此在實際上，個人主觀不受限制之事先同意，仍可排除法律規範的客觀保護，或直接使其失去產生限制行為作用之效力[103]。而此一觀點看似與客觀規範效果對立，但其依據在於每個人都是單一自主個人的資料保護主體，所以被保護的主體自然有自我決定是否同意他人使用其個人資料的自主權[104]。既然每個人都是個人資料的擁有者，自然每個人的主觀意志，皆不可加以限縮[105]。雖然追蹤 App 下載前會徵詢用戶授權與否，但防疫主管官署通常會將合法授權範圍極大化，同時也會連結對於用戶不一定具實際用途的數位服務功能，這些功能或許對特定受眾群有其實用性，但其功能卻能協助服務提供平台或機構，在被授權延長的時間及擴大讀取的內容範圍中，儲存更多個人資料，並在提供服務的定型化合約條款的規定架構下，以履行合約為前提盡可能地加以使用[106]，因此不無違反歐盟《一般資料保護規則》第 5 條第一項所示「目的連結」、「依忠實與信賴處理」及「儲存限制」原則之疑慮。目前學界也有許關於追蹤 App 涉及資料運用的討論，有見解從「儲存限制」之使用原則加以延伸，其指出，即便人民事先同意讓行政機關在合法基礎下，以合目的性之行為，將系統蒐集之個資儲存於資料庫中，但不得以此反推可知之個人自主意願，將個資移作其他不合目的之用途。而防疫主管官署也應以無法回推之「匿名化」（Anonymisierung）格式，或至少以暫時遮蔽身分識別之「假名化」格式儲存個資，方能符合行政

102 Art. 6 Abs. 1 Buchst. b DS-GVO; § 22 Abs. 1 BDSG; Samardzic/Becker (Fn. 47), S. 648.

103 Samardzic/Becker (Fn. 47), S. 648.

104 Yoan Hermstrüwer, Informationelle Selbstgefährdung, 2016, S. 21-31 ff.; Philip Radlanski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 204-209 ff.

105 Buchner/Petri (Fn. 57), Rn. 17.

106 Art. 6 Abs. 1 S. 1 Buchst. b DS-GVO; Samardzic/Becker (Fn. 47), S. 648.

機關保護人民、且機關自己不為惡之忠實與信賴原則[107]。

從用戶的角度而言，「事先同意」要件之優先性，對其個人資料保護常常產生強烈的矛盾與反差，因個人為了防疫必要，雖然同意授權 App 使用個人資料，但一般用戶對個人資料保護仍有高度的期待。多數用戶在歷經歐盟《一般資料保護規則》生效的這段時間後，都認知到歐盟《一般資料保護規則》的嚴格規定，以及法條中提供的高度保護程度，甚至連毫無損害性之幼兒園或中小學畢業紀念相片，在未經當事人或法定代理人同意前，亦不得使用[108]。於此同時，追蹤 App 的用戶也會體認到一個事實，即使歐盟及德國對於個人資料的儲存與處理具有相當嚴格的規定，但各大社群及線上數位平台多為美國企業，他們在技術上早已掌握個人的行動資訊及相關個資，因此嚴格的法律規定雖有部分規範效果，但在實務上，卻無法對此類跨國企業產生實際限制，規範強度也相對較弱。而讓法規範對社群平台企業拘束力降低的原因，可能之因素也在於個人「事先同意」的效力範圍無限擴大，而個資保護機關得以維護個人人格權及隱私權為由而阻擋的能力卻偏低，以致於「事先同意」幾乎可適用任何處理個人資料的需求，而此一「事先同意」與「個資保護」之間的矛盾，也不斷出現在防疫追蹤 App 的使用過程中[109]。

目前社會大眾儘管有意識到如何保護個資不受追蹤 App 過度利用之急迫性，但經由用戶事先自願同意取得之匿名資料，其後續處理中如何防止外洩或濫用並非易事，所以在「事先同意」效力過於廣泛的情況下，為免個資因防疫主管官署恣意行政處分而有保護不全之闕漏，因此在符合目的及合法性原則下，仍應「依忠實與信賴處理」（Verarbeitung nach Treu und Glauben）[110]原則處理個資，僅將個資用於最必要、對民眾最有利，且傷害

107 Samardzic/Becker (Fn. 47), S. 648; Art. 5 Abs. 1 Buchst. e Hs. 2. und Art. 17 Abs. 1 Buchst. a DS-GVO.

108 Samardzic/Becker (Fn. 47), S. 648.

109 Samardzic/Becker (Fn. 47), S. 648.

110 Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 Buchst. a und Art. 7 Buchst. f DS-GVO.

風險最低之防疫措施，並且不隨意擴張使用範圍，以免違反此一原則[111]。德國聯邦眾議院科學機構（Wissenschaftlichen Dienstes des Bundestages）在立法前之公開諮詢中，針對新冠病毒大流行時期，「行動電話追蹤」（Handy-Tracking）是否適合用於控制接觸感染的爭議，曾依據德國《聯邦資料保護法》及歐盟《一般資料保護規則》之立法衡量理由，在 2020 年 4 月 22 日提出公開意見。其以為，民眾係自願使用追蹤 App，且只有匿名的資料被處理，因此並不違反歐盟及德國內之資料保護法規，亦不會有個資濫用之疑慮[112]。與此相同的還有歐盟執委會為研擬《行動-App 指引》（Leitlinien zu „Mobile-Apps“）草案，在 2020 年 4 月 16 日的官方文件中，亦列入並強化資料保護之機制[113]。

3. 追蹤 App 於實際應用產生的爭議

3.1 「事前同意」造成健康權與資訊自主權間的歧異

基於不斷上升的感染及確診人數，許多科技產業為因應防疫，也紛紛採取 App 等各類科技預警或防治措施，以保護旗下員工、顧客及其家屬免受病毒危害。但是各類的科技工具難免都會運用敏感醫療及健康資料，例如發燒檢測資料、身體狀態資料填覆表格等，並於納入資料庫後分析處理或介接至

111 Samardzic/Becker (Fn. 47), S. 648 f.

112 Wissenschaftliche Dienste (2020), Einzelfragen zum Handy-Tracking in Deutschland im Zusammenhang mit der Corona-Pandemie – Ausarbeitung, Deutscher Bundestag, online verfügbar unter https://www.bundestag.de/resource/blob/692998/c88738c96c087f66748ac75a0a7788b2/WD-3-098-20-pdf-data.pdf (zuletzt geprüft am Mär. 29, 2021); Samardzic/Becker (Fn. 47), S. 648 f.

113 Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie, Europäische Kommission, online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN (zuletzt geprüft am Mär. 29, 2021); Samardzic/Becker (Fn. 47), S. 649.

其他醫療用資料庫[114]。對於公、私部門而言，如何兼顧個人隱私權及第三人身體健康權間之平衡，已成為必須即刻處理的難題。換句話說，如何在公共衛生及醫療考量下，避免逾越個人資料保護法制之允許範圍[115]。不同政府機關對於科技工具蒐集與處理個資的見解不同，而目前私部門對於新冠病毒造成的影響，若採用傳統防疫措施，無法有效克服感染的擴大，但特種個資蒐集、使用及處理之合法性，仍有待必要的檢測[116]。依據歐盟《一般資料保護規則》第 9 條第一項及第二項第 a 款[117]之規定，醫療、健康狀態及病毒檢測結果等資訊，均屬敏感性個資，而此類敏感性個資除非符合例外條款的規定，否則原則上，非本人同意是禁止被蒐集與處理[118]。在疫情擴散期間，防疫及阻擋病毒擴散的緊急措施，常被用來當作使用個資的合理目的，但依《一般資料保護規則》第 9 條第二項第 a 款[119]規定，除利害關係人針對特定或多項確定目的，明確表示同意其敏感個資之處理，第三人方得處理敏感個資。但同款後段也有明確之例外規定，若歐盟法或各成員國國內法完全禁止本人自願事前授權之法律效力，則第三人即使取得本人自願事先授權，亦不得處理當事人之敏感個資[120]。此處之例外規定相較於同款前段阻卻違法要件之限制程度更高，連本人之自願都不得授權他人使用特種個資，與歐盟《一般資料保護規則》第 9 條規定[121]之特種個資禁用原則一致，但仍須以其他歐盟法或成員國國內法為依據[122]。換句話說，其他歐盟法或成員國國內法可以更嚴格之禁止規定限制特種個資使用，但不得制定更寬鬆或模糊之法律，以

114 Rath/Feuerherdt (Fn. 18).
115 Rath/Feuerherdt (Fn. 18).
116 Rath/Feuerherdt (Fn. 18).
117 Art. 9 Abs. 1, 2 Buchst. a DS-GVO.
118 Rath/Feuerherdt (Fn. 18).
119 Art. 9 Abs. 2 DS-GVO.
120 Rath/Feuerherdt (Fn. 18).
121 Art. 9 DS-GVO.
122 Rath/Feuerherdt (Fn. 18).

免除歐盟《一般資料保護規則》第 9 條第一項及第二項[123]之適用。

另於歐盟《一般資料保護規則》第 9 條第二項第 b、c 款[124]中，亦有相關類似之例外規定，敏感個資之蒐集、處理及後續使用，都必須事先獲得利害關係人依自由意願表示之同意，或符合其他法定例外之要件，方得為之[125]。整體而言，歐盟《一般資料保護規則》第 9 條第二項[126]規定之例外要件，雖目前處於防疫期間，但考量例外規定之特殊性，仍應加以嚴格解釋及界定，且不能當作介入個人隱私領域的特許證[127]。

然而敏感個資的處理，目前不能在未區分的情況下，一昧全部適用歐盟《一般資料保護規則》第 9 條第二項第 g 款[128]為保護顯著公眾利益，而例外允許處理敏感個資之規定。儘管如此，歐盟的立法者在制定《一般資料保護規則》時，曾預想重大傳染病大流行時的個資處理規範，在歐盟《一般資料保護規則》的第 46 點立法理由中即有相關說明，為監控疾病大流行的狀況，得例外允許處理敏感個資[129]。但此一立法說明承認的例外，仍須落實到各成員國，換句話說，各成員國的立法者必須意識到預防疾病大流行的風險，並將歐盟《一般資料保護規則》所第 9 條第二項規定之上位規範，以立法方式具體實踐，賦予敏感個資於防疫期間使用之合法性。德國政府雖意識到新冠病毒大流行期間，為使用科技工具防疫必然會使用到一般及敏感個資，但行政及立法機關並未提出明確、具體的法案，以至於敏感個資在防疫期間，是否能依據歐盟《一般資料保護規則》第 9 條第二項第 g 款[130]例外准予蒐集及處理，尚無直接法源[131]。

123 Art. 9 Abs. 1 bis 2 DS-GVO.
124 Art. 9 Abs. 2 Buchst. a bis c DS-GVO.
125 Rath/Feuerherdt (Fn. 18).
126 Art. 9 Abs. 2 DS-GVO.
127 Rath/Feuerherdt (Fn. 18).
128 Art. 9 Abs. 2 Buchst. g DS-GVO.
129 Rath/Feuerherdt (Fn. 18).
130 Art. 9 Abs. 2 Buchst. g DS-GVO.
131 Rath/Feuerherdt (Fn. 18).

實際上，敏感健康或醫療資料之處理，在部分領域確實有其必要性，例如依歐盟《一般資料保護規則》第 9 條第二項第 b 款[132]之例外規定，若基於行使勞動及社會法賦予之權利與義務所需，則僱傭關係中，即可允許使用敏感性個資。在此之中，自然還包括勞動法規定雇主對所有勞工的照護義務，由此推斷，若雇主為保護企業員工不被新冠病毒感染，或為避免病毒於員工群聚下造成擴散而處理員工之敏感健康個資，符合歐盟《一般資料保護規則》第 9 條之要件，所以雇主可制定相關防疫措施，例如疾病通報、薪資提前給付及部門同事間對發生感染症狀者之回報[133]。此外，針對其他處理敏感健康個資例外要件所需的事前同意，在防疫實務上，不應過度主張，應有一定程度的鬆綁。因此歐盟《一般資料保護規則》第 9 條第二項第 c 款[134]允許在保護生命等重要利益時，第三人得處理敏感個資，但此一例外生效的前提在於，利害關係人係處於無法自行同意並授權的狀態下，例如當事人精神或身體重病，抑或因治療無法依照自由意志表示授權。除此之外，雇主欲以第三人身分處理員工之敏感個資，仍須個別徵求員工之事前同意[135]。關於勞雇關係中，雇主得否強制要求員工安裝追蹤 App 之爭議，則另論於本文第 4 節。

3.2 從消費者保護法觀點論「事先同意」之漏洞

追蹤 App 使用個資雖係自願，且經事先同意授權，第三人（政府機關、產業或個人）可處理個人資料，但可使用的資料類型、性質及範圍並無明確之列示規定，因此尚有爭議及亟待釐清之處。其中包括個人醫療健康資料、位置資料、溝通資料及其他個人接觸相關資料等，基於「事先同意」的宣示授權效力，其於資料保護法律規定的適用上，不能毫無限制、一體適用，否則將過於輕率。此一問題雖有爭議，但目前逐漸從《消費者保護法》之論點

132 Art.9 Abs. 2 Buchst. b DS-GVO.
133 Rath/Feuerherdt (Fn. 18).
134 Art.9 Abs. 2 Buchst. c DS-GVO.
135 Rath/Feuerherdt (Fn. 18).

發展出，對「事先同意」授權使用的合法效力應有必要限制之論點[136]。此一合法性考量，特別是在「事先同意」被列入契約條款，當作當事人約定事項之一時，而其漏洞造成潛在的風險程度，更高於「事先同意」授權使用個資的便利性與實用性[137]。有鑑於此，德國立法者針對消費者保護制定多重的規範，同時也認定法律規定不能造成對消費者不利的狀態，亦不得與保護消費者的原意背離，因此在契約中雙方約定之條款雖有同意授權使用個資之規定，但若與消費者權益保護原則相違，則可依據德國《民法》第 241a 條第三項、第 312k 條第一項、第 361 條第二項、第 487 條、第 512 條、第 650o 條及第 655e 條視為無效[138]。由此可知，消費者透過法規的保護機制，仍可在違反其已對外宣示之意願（例如事先同意授權）的情況下，受到大幅度的保護，除德國《民法》外，此一原則也援引自歐洲《消費者保護法》（Verbraucherschutzrecht）[139]。

若將個人資料保護的規範意涵，引用消費者保護的概念來對比及理解，可發現兩者在法律的適用方式接近，類推前述德國《民法》及歐洲《消費者保護法》為擴大消費者保護，而對「事先同意」授權效力的限縮，則對個人資料處理的事先同意效力，亦因限縮於不損害個人隱私與人格權保障之範圍內。就歐盟《一般資料保護規則》第 4 條至第 6 條[140]規定而言，對事先同意授權效力的限制，較弱於德國《民法》規定，也缺乏與歐洲《消費者保護法》相等之限制性規定[141]。與此相反的，歐盟《一般資料保護規則》在其基於保護個人資料於處理過程不會遭致他人濫用的限制性規定中，則係以徵詢事先同意，作為解除限制規定的阻卻違法要件。此要件不單是針對一般個人資料的處理，連同具有機敏性特種個資也包括在內，如歐盟《一般資料保護

136 Samardzic/Becker (Fn. 47), S. 650.
137 §§ 241a III, 312k I, 361 II, 487, 512, 650o, 655e BGB.
138 §§ 241a III, 312k I, 361 II, 487, 512, 650o, 655e BGB.
139 Samardzic/Becker (Fn. 47), S. 650.
140 Art. 4, Art. 5, Art. 6 DS-GVO.
141 Samardzic/Becker (Fn. 47), S. 650; Schulz (Fn. 100), Rn. 1.

規則》第 9 條第一項[142]規定禁止處理之種族或民族血緣背景、政治意見、宗教及世界觀認同、工會成員身分、基因資料、生物資料、個人識別資料、自然人之健康、性生活及性取向資料等，但同時於同條第二項第 a 款[143]規定中，卻僅以取得事先同意之表示為例外條款，提供阻卻違法要件以解除同條第一項禁止規定之限制[144]。

3.3 AI 與大數據對個人行為的側寫

追蹤 App 透過蒐集及使用用戶之一般與特種個資達到防疫目的，但其後台系統功能在執行時，則涉及被歐盟法禁止之 AI 演算法連結大數據進行個人行為側寫（Profiling-Daten）。歐盟《一般資料保護規則》第 22 條第二項第 c 款[145]規定，將個人側寫資料的處理，同樣列入需要相關人明確表述事先同意授權使用個資的範圍中。此一規定，也適用在歐盟成員國外之其他國家的資料傳輸與處理[146]。儘管「事先同意」作為阻卻違法要件有其漏洞，但歐盟《一般資料保護規則》第 22 條第三項及第四項規定[147]對於 AI 處理大數據資料，特別是對個人行為偏好之「側寫」（Profiling），則要求涉及個人健康醫療資料處理時，應採取保護個人權利、自由及相關人利益之適當措施。例如針對由 AI 或機器人系統自動產生之決策結果或各類案件之決定，處理

142 Art. 9 Abs. 1 DS-GVO, „Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt."

143 Art. 9 Abs. 2 Buchst. a DS-GVO.

144 Samardzic/Becker (Fn. 47), S. 650; Alexander Schiff, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, § 9 Rn. 33 ff.

145 Art. 22 Abs. 2 Buchst. c DS-GVO.

146 Jörg Hladjk, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, § 22 Rn. 12, 15; Samardzic/Becker (Fn. 47), S. 650.

147 Art. 22 Abs. 3, 4 DS-GVO.

個人資料之企業或機構，應建置救濟機制或管道，供利害關係人就系統自動產生之決定提出異議或不服之申訴[148]。

關於禁止資料傳輸之規定，因缺乏充分、適當之保障機制，以至於依歐盟《一般資料保護規則》第 49 條第一項第 a 款[149]所規定之事先同意表述，即可有效阻卻違法[150]。在前述的案例狀況及可能產生的個資風險因素中，都與「事先同意」授權使用個資的規定有關，但鑑於個資在數位產業發展的優勢及個人隱私權的衝突，歐盟《一般資料保護規則》可能為立法者的政治妥協結果，而其中第 4 條第十一款、第 6 條第一項第 a 款及第 7 條[151]，在立法前後，都具有相當之爭議[152]。舉例來說，處理前，應「清楚且確實」徵詢「事先同意」的個人資料，不該僅限於具敏感性之個人資料（例如疫苗注射紀錄、確診者隔離及就醫病歷等），需要「清楚且確實」徵詢「事先同意」的個人資料處理，應含括所有種類的個人資料，不論是否為敏感性個人資料。但是，此一防止個人資料因不夠明確之事先同意而導致的風險機制，並未在歐洲議會的立法程序中被全面納入考量[153]。

從完整保護個人隱私及人格權的觀點來看，明確的「事先同意」作為阻卻違法要件的機制，應儘量廣泛適用於各類個資蒐集與處理，同時，有效「事先同意」的條件，亦應儘量簡化，使其容易遵守，讓資料流通在合法範圍內，減少其限制。在此目的中，自然也包括透過「事先同意」形成對有保障價值之特殊、敏感性資料，如健康醫療資料等的保護機制，特別是各類資料的連結或傳輸，像是 AI 連結大數據對個人行為偏好的判斷與預測，必須加以嚴格的限制，但各個國家間的一般個資傳輸，則只應設計法定最低保護

148 Hladjk (Fn. 146), Rn. 12, 15; Samardzic/Becker (Fn. 47), S. 650.

149 Art. 49 Abs. 1 Buchst. a DS-GVO.

150 Samardzic/Becker (Fn. 47), S. 650.

151 Art. 4 Nr. 11, Art. 6 Abs. 1 Nr. 1 Buchst. a, Art. 7 DS-GVO.

152 Gierschmann/Schlender/Stentzel/Veil (Fn. 64), Rn. 37.

153 Samardzic/Becker (Fn. 47), S. 650; Lutz Schreiber, in: Plath (Hrsg.), DSGVO/BDSG Kommentar, 3. Aufl., 2018, § 4 Rn. 41.

門檻，減少流通障礙，讓個人資料在低風險的範圍內自由流通，促進資料經濟發展[154]。至於透過健康醫療資料進行的行為預測（資料側寫），依歐盟《一般資料保護規則》第 22 條第四項[155]之規定，原則禁止，但可經由關係人之明確同意表述而以例外條款阻卻違法。歐盟法將大量個人資料保護標準，用此一與消費者保護原則對立之阻卻違法要件作為例外使用，應為未充分考慮消費者保護原則用以防止例外條款對個資濫用風險預防機制情況下的政治判斷[156]。「事先同意」作為阻卻違法要件，也被類推適用於防疫追蹤 App 的個人資料使用與處理。雖然 App 在下載與安裝時已徵詢用戶之書面明確事先同意授權處理個人資料，但被傳輸及處理的個人資料種類、範圍、儲存地點及疫情後的使用等，並未有清楚的說明，以致尚有疑慮[157]。

在歐盟《一般資料保護規則》第 9 條第二項第 a 款[158]則有原則禁止，但例外允許（Verbot mit Erlaubnisvorbehalt）之規定，其中事先同意授權的要求及範圍，則明顯為政治妥協的結果。另依據歐盟《一般資料保護規則》第 9 條第四項[159]之保留條款可知，歐盟本身及成員國可針對不同種類個人資料之事先同意要件效力，自行訂定限制性規定、不同程度之標準或額外之條件[160]。因此，在防疫期間，追蹤 App 的投入雖然會連結具機敏性之個人醫療資料，但只要歐盟或各會員國基於其防治新冠病毒的必要性及急迫性，並考量各成員國內之病毒散布狀況，則各國立法者仍有可能經由立法或修法，在不需經過個人書面同意得情況下，由法律規定將個人醫療資料的處理權限保

154 Gierschmann/Schlender/Stentzel/Veil (Fn. 64), Rn. 48 f.; Samardzic/Becker (Fn. 47), S. 650.

155 Art. 22 Abs. 4 DS-GVO.

156 Hladjk (Fn. 146), Rn. 13; Gierschmann/Schlender/Stentzel/Veil (Fn. 64), Rn. 83.

157 Samardzic/Becker (Fn. 47), S. 650.

158 Art. 9 Abs. 2 Buchst. a DS-GVO.

159 Art. 9 Abs. 4 DS-GVO.

160 Datenschutz.org (Nov. 18, 2022), Verbot mit Erlaubnisvorbehalt im Datenschutzrecht, online verfügbar unter https://www.datenschutz.org/verbot-mit-erlaubnisvorbehalt/ (zuletzt geprüft am Dez. 18, 2022).

留給特定機關（例如衛生部或特定防疫研究機構），使該機關可快速利用個人醫療資料，以 App 或其他科技工具執行防疫工作[161]。雖然防疫著重迅速，但若以法律直接授權行政機關或特定機構便宜行事，則個人醫療資料的機敏性很可能遭到破壞，在疫情結束或無防疫需求時，此等醫療個人資料之後續保存或銷毀並無法定追蹤機制，社會大眾或個人根本無法追蹤，故此等資料具有經濟價值，可能導致濫用的發生[162]。

綜合上述觀點來看，目前歐盟《一般資料保護規則》對於追蹤 App 在防疫上的應用並無專屬篇章或特定條文加以規定，所以個人對 App 處理個人資料之事先同意效力並無任何限制[163]。目前歐盟《一般資料保護規則》對個人資料處理的阻卻違法係以例外條款之「事先同意」授權為要件，但依歐盟《一般資料保護規則》第 9 條第二項第 h 款及第三項[164]規定，「事先同意」之阻卻違法要件並不適用於醫療專業人員處理之具機敏性個人資料，故此等法定之醫療專業人員對敏感個資之處理，並不受到「事先同意」的限制，故醫療專業人員若係依法從事業務而使用追蹤 App 蒐集之個人資料，即使事先未得到個人明確表示之同意授權，仍可適用例外條款，合法處理個人資料。儘管，醫療專業人員不一定受行政機關委託處理個人資料，抑或此等專業人員僅將個人資料用於醫學學術研究，但在未有預防濫用機制的情況下，仍難以消除大眾之疑慮[165]。另外，歐盟《一般資料保護規則》並未以專長或證照資格為條件，「事先同意」可授權於任何受歐盟《一般資料保護規則》規範之自然人或法人，而且對於「事先同意」並無職業保密（沉默）義務或使用者之專業知識等條件[166]，故由此推論可知，任何私人企業、機構或個人均能以簡易的方式取得相關人之「事先同意」，並在符合歐盟《一般資料保護規

161 Datenschutz.org (Fn. 160).
162 Samardzic/Becker (Fn. 47), S. 651.
163 Samardzic/Becker (Fn. 47), S. 650.
164 Art. 9 Abs. 2 Buchst. h, III DS-GVO.
165 Samardzic/Becker (Fn. 47), S. 650.
166 Samardzic/Becker (Fn. 47), S. 650.

則》規定之前提下，自行研發並提供防疫用途之追蹤 App。

3.4 追蹤 App 作業系統透明度不足之疑慮

「羅伯特科赫研究所」開發的追蹤 App 係採用開源碼（Open Source）進行程式設計，所以外部技術人員都可以檢視 App 的程式編碼或演算法，同時追蹤 App 也依據歐盟《一般資料保護規則》第 35 條[167]規定之要求，執行資料保護風險評估（Datenschutz-Folgenabschätzung），並已公開評估結果，本條之規定也是歐盟《一般資料保護規則》第 5 條第一項「透明度」（Transparenz）[168]原則在 App 或 AI 演算法應用層面之具體落實。當 App 系統運作程序及使用個資範圍具「透明度」，則社會大眾也會因不確定感減少，隨之提高其接受度。而德國駭客組織「混沌電腦俱樂部」（Chaos Computer Club）及公民團體 「資訊人員和平及社會責任論壇」（Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung, e.V., FIfF），則以自行完成之資料保護風險評估說明追蹤 App 的高風險，特別是面對駭客攻擊時，App 本身的資安防護力不足[169]。因追蹤 App 本身並非獨立之作業系統，其主要運作架構，係依靠 Google 及 Apple 的「曝光通知系統」（Exposure Notification System），來記錄用戶個人接觸他人的歷程。而追蹤 App 的系統只是行動電話或行動裝置作業系統的一部分，因此「羅伯特科赫研究所」並不能修正或調整行動電話或裝置之作業系統，只能配合使用，在此狀況下之資料保護風險評估也發現，防疫主管機構無法觸碰、修正或調整的系統部分，根本就是一個黑盒子，外界無法得知此裝置之系統如何儲存、傳輸及處理個資，以及 Google 及 Apple 的平台是否將這些裝置作業系統蒐集而來的個資介接至其他資料庫，或做其他商業營利使用（例如大數據之精準行銷）[170]。

---

167 Art. 35 DS-GVO.

168 Art. 5 Abs. 1 DS-GVO.

169 FIfF (Fn. 96); Kötter (Fn. 7).

170 Karolin Dörner (Jul. 17, 2020), Corona-App: Wissenschaftler Kritisieren Rolle von Google

儘管如此，對於 Google 及 Apple 並無高風險之評估結果，所以社會大眾至少對於這兩大平台在個資保護作為的信任度仍高，故對兩大平台使用其個資的容忍度也相對較高。換句話說，當用戶個人使用 Android 或 iOS 行動電話及裝置時，即表示信任平台業者生產之裝置，以及容忍使用行動電話或裝置可能提高的個資風險[171]。通常此類風險的出現多來自於用戶使用搭配平台業者作業系統的行動電話或裝置，處理與個資相關之事務。而用戶明知平台業者在行動電話或裝置運作時，他們的個資可能被傳輸至平台資料庫或作為其他用途，但仍繼續使用，則此舉也接受平台對其個資的使用，甚至會為了方便使用平台提供之數位服務，而自行配合改變使用習慣，但爭議的是，平台並未說明個資實際使用的狀態[172]。

就實務層面而言，追蹤 App 只是以既有 Google 及 Apple 提供的數位平台基礎，並以 Android 及 iOS 作業系統支援該 App 的開發與應用，所以不論是一般或特種個資，均無法排除 Google 及 Apple 之蒐集、儲存、傳輸及處理。然而依據歐盟《一般資料保護規則》執行資料保護風險評估之結果，卻認定兩大平台具一定程度信任度，其原因並非兩大平台真如同對外宣示者，不會將所蒐集之個資作為目的外之使用[173]。而是因為現有智慧型行動電話或各類行動裝置，幾乎都是內建使用 Android 及 iOS 作業系統，以及支援該兩大平台系統的 App 開發環境，所以甚難找到比 Google 及 Apple 更具信任度之數位服務供應平台，所以在沒有其他替代可能性的情況下，其風險評估可比較的對象少，加上社會大眾多數非資訊技術專家，很難改用不熟悉及不相容的作業系統，所以對比下自然呈現偏高之可信度[174]。

另外，追蹤 App 功能是否發揮的關鍵在於安裝、使用的人數，若使用人

---

und Apple, MDR Missen, online verfügbar unter https://www.mdr.de/wissen/Corona-warn-app-einschaetzung-leopoldina100.html (zuletzt geprüft am Aug. 2, 2020).

171 Dörner (Fn. 170).

172 Dörner (Fn. 170).

173 FIfF (Fn. 96); Kötter (Fn. 7).

174 FIfF (Fn. 96); Kötter (Fn. 7).

數多，則透過行動裝置偵測距離並判斷是否與確診者接觸的準確度才會提高，若使用人數過少，則 App 用戶產生的識別訊號，無法與確診者用戶的訊號於近距離接觸進行比對，並即時反應，將導致誤判或該判而未判斷的偏差率增高。為使安裝使用率提升，「羅伯特科赫研究所」必然只能採用使用人口最多之 Android 及 iOS 作業系統，不可能耗費成本尋求替代系統或另自行開發[175]，因此在採用 Google 及 Apple 平台提供之作業系統與相容介面幾乎不可避免，然而，即便大眾對兩大平台的信任度相對較高，但不表示平台業者可以商業機密為理由，長期維持其作業系統的黑箱運作，拒絕公開用戶個資傳輸、儲存與使用方式，以及後續完整之處理流程。社群或數位平台營運業者，雖因商業營利而有維持營業秘密之必要，但面對個人隱私、公眾信賴及社會公益，仍應適用歐盟《一般資料保護規則》課予落實「透明化」原則之義務。

3.5 追蹤 App 成為民眾「社會參與」門檻的影響

儘管聯邦政府以自願方式鼓勵大眾安裝使用追蹤 App，但是卻有民眾主動要求應將安裝使用追蹤 App 當作社會參與的條件，也就是作為個人從事社交活動或進出公眾場所的要件。但單一個人的社會網絡可能相當廣闊，任何人參與任何社會活動不一定是有特定目的，所以有時候是規律進行，例如每日上下班出勤，有時候是休閒娛樂，所以地點與時間不固定[176]。但若以安裝追蹤 App 作為社會參與的條件，除不願意安裝者將被排擠於社會之外，更會造成人與人間之猜忌與對立，並造成恐懼地蔓延，因為人人皆須以 App 證明自己未接觸確診者，所以無感染危險。即使病毒並未擴散，但因追蹤 App 推出，反而讓健康但不願安裝使用的人，陷入被社會壓迫或歧視，間接侵害這

175 Kötter (Fn. 7).

176 Deutscher Gewerkschaftsbund (Jun. 19, 2020), Corona-App und Arbeitsrecht: Was darf mein Chef, Deutscher Gewerkschaftsbund (DGB), online verfügbar unter https://www.dgb.de/themen/++co++958547b4-b236-11ea-a4c5-52540088cada (zuletzt geprüft am Aug. 19, 2020); Kötter (Fn. 7).

些人的人格權、隱私權、行動自由及資訊自主等重要人權[177]。「羅伯特科赫研究所」從技術與應用層面也認為，其實德國還有不少的國民未使用行動電話，或未持有與追蹤 App 相容的行動電話或裝置，尤其是小孩、年長者及貧窮階層，難以擁有行動電話或裝置，若以追蹤 App 作為社會活動參與門檻，則有相當多的經濟弱勢族群被排擠於社會資源分配之外。另現狀還顯示出，不單經濟問題，還包括社會背景及名譽（擔心被人認為有確診者或疑似感染者進入）等因素，導致私人機構以追蹤 App 作為接受申請或提供社會協助的條件，反而大量排擠真正需要受到保護之國民[178]。

倡議以追蹤 App 作為社會參與條件者之觀點也引起追蹤 App 在特定社會結構是否具有實際效用的爭論，因為老年、孩童及社會經濟弱勢者不一定擁有行動裝置，故有很高之比例無法使用追蹤 App，也不能透過 App 防疫或接觸確診者後進行居家隔離，以至於被認為是較易遭感染的危險族群[179]。此類言論目前並無定論，但很明顯的，追蹤 App 的使用在私人領域，對許多人而言，也會視正反兩面之壓力而不得不安裝使用。支持者認為，追蹤 App 是很便利的防疫措施，符合自利及他利的需求，但反對者也認為，儘管追蹤 App 便於防疫，但須思考的還有許多可能政策推動未考量到的狀況，例如尚有許多社會邊緣群體長期被邊緣化，根本未享用社會資源，以至於他們無法如同中產階級可在行動裝置上安裝追蹤 App 防疫，即使這些人有工作，企業雇主可能也只提供員工公務用行動電話，故只有在值勤時才有防疫的作用[180]。

鑑於民眾可能會因追蹤 App 的安裝使用來區隔危險或不危險的族群，以致社會弱勢族群容易遭受歧視而損害其平等權，故「羅伯特科赫研究所」為防止不理性之社會壓力形成對弱勢的壓迫，不對外公開個人安裝使用追蹤 App 之狀態，亦不讓外界查詢使用者資訊。只要用戶不主動對外界公開其是

177 Deutscher Gewerkschaftsbund (Fn. 176); Kötter (Fn. 7).
178 Kötter (Fn. 7).
179 Westenthanner/Humpa (Fn. 8); Kötter (Fn. 7).
180 Deutscher Gewerkschaftsbund (Fn. 176); Kötter (Fn. 7).

否有安裝追蹤 App，則 App 的使用並無法被檢視或偵測。不論是行政機關（例如聯邦衛生部），或是第三人（例如用戶之雇主或同事），從行動裝置外部均無法審視該裝置是否有安裝過追蹤 App，亦無法得知 App 的功能曾被完全使用過[181]。而此類安裝使用追蹤 App 的個資並無公開的法源依據，所以非經本人自願同意，「羅伯特科赫研究所」亦不得公開或作為非防疫之用途。現階段須注意的是，一般人進入特定私人場所仍有可能被要求出示使用中的追蹤 App，或以 App 顯示近期陰性採檢結果，以作為入場之條件。但因目前並無法律禁止以追蹤 App 作為營業或私人場所的入場條件，以致於安裝 App 雖屬自願，但為了進入社會生活圈，很多非自願者也只能同意安裝，但實際上並非依其自由意願的而同意安裝使用[182]。則此時的自願安裝行為，不等同自由意願下之事先同意授權，故 App 對個資的使用將有違反歐盟《一般資料保護規則》第 7 條第四項及第 9 條第二項[183]規定之疑慮。

4. 追蹤 App 於工作場域的落實與推動條件

4.1 雇主要求員工安裝使用追蹤 App 之判斷標準

一般民眾不論是否為企業員工，在手機或載具上安裝追蹤 App 後，系統將會自動偵測使用者是否與他人接觸時，是否達到可能的傳染時間，或保持充分之距離，而所有的資料都是經過藍芽系統進行交換，若用戶日後經採檢確診，則可自行決定個人確診的資訊是否可經由追蹤 App 讓其他用戶比對，藉此提早發出警示並保持安全社交距離。而近距離接觸者獲得警示後，也可自行決定通報、隔離檢疫並由醫療院所採檢[184]。聯邦政府強調 App 由市民自願並經由事前同意後安裝、使用，但不論是經由緊急立法修正後的《傳染病

181 Kötter (Fn. 7).

182 Bundesregierung (Fn. 4); Kötter (Fn. 7).

183 Art. 7 Abs. 4, Art. 9 Abs. 2 DS-GVO.

184 Michael Fuhlrott, Corona-Warn-App: Nutzungspflicht für Arbeitnehmer?, GWR 2020, S. 270 (275 ff.); Thomas Köllmann, Die Corona-Warn-App, NZA 2020, S. 831 (831 ff.).

防治法》，或是現行勞動法規目前尚無法律授權雇主強制勞工安裝追蹤 App 的依據。相對於企業而言，如果能預防病毒在其工作場域擴散及減緩疫情之嚴重化，對其企業營運及社會形象有整體的正面效應。對此，雖曾有國會議員建議修法，並支持「消費者問題專家諮詢會議」（Sachverständigenrat für Verbraucherfragen, SVRV）對聯邦司法部（das Bundesjustizministerium）[185]修法賦予企業雇主強制要求員工基於防疫目的安裝追蹤 App 法源之建議[186]，但最終仍未採行，因為員工如能自願安裝追蹤 App 爭議最低，且對企業更為有利。然而，若員工並非都自願下載安裝時，企業面臨的問題就是能否以雇主的身分要求員工在其私人或公用行動裝置上，安裝並開啟追蹤 App。單就私人行動電話或裝置來看，員工完全無須遵守企業的要求，因為私人行動裝置屬於員工私人財產，任何來自企業對於員工私人財產的介入都是違法的，且員工不需要忍受私人財產的使用被企業干預。另外，相對於企業經營者，員工對雇主並無義務經由安裝、使用追蹤 App 來保護自身健康及工作體力之法定義務[187]。

但企業若是要求員工在公用行動裝置上安裝並使用追蹤 App，則員工不一定能如同支配私人財產般，加以拒絕。因為一方面該行動裝置之財產權屬於企業，另一方面，員工使用該公用行動裝置之時間多於公務或上班時間，可能與其他同事處於室內或接近之範圍，故而關係他人之健康保護。特別是

185 Susanne Dehmel/Peter Kenning/Gert G. Wagner/Christa Liedtke/Hans W. Micklitz/Louisa Specht-Riemenschneider (2020), Die Wirksamkeit der Corona-Warn-App wird sich nur im Praxistest zeigen, Sachverständigenrats für Verbraucherfragen, S. 23 ff., online verfügbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Fachinformationen/PolicyBrief_Corona_APP.pdf?__blob=publicationFile&v=2.

186 Fuhlrott (Fn. 184), S. 275 ff.; Köllmann (Fn. 184), S. 831 ff.

187 Christiane Schulzki-Haddouti (Nov. 3, 2020), Medizinische Hochschule Hannover und Ubilabs entwickeln Corona-App, Heise Online, online verfügbar unter https://www.heise.de/newsticker/meldung/Medizinische-Hochschule-Hannover-und-Ubilabs-entwickeln-Corona-App-4680487.html?seite=all (zuletzt geprüft am Jun. 1, 2020); Rath/Feuerherdt (Fn. 18).

勞動法上企業雇主必須保障員工健康，而員工間也需相互維護對方之健康，所以公用行動裝置受到企業要求安裝追蹤 App 的必要性比私人行動裝置還高[188]。即使在此種情況下，基於資料保護法規的嚴格規定，企業內部對公用行動電話安裝追蹤 App 的要求，仍常造成雇主與員工間的爭議。在實務上，很多企業員工雖然使用公用行動裝置，但難免會用於私人領域或作為私人聯繫通訊之用，同時也會存有涉及個人隱私之圖文或影音個資，甚至是敏感個資，一旦企業強制員工安裝追蹤 App，無疑也是高度介入員工之隱私與私人生活領域，因此員工並無忍受被企業干預隱私的容忍義務[189]。在大多數的案例中，企業雇主並無法源依據直接要求員工安裝 App，所以只能以道德方式呼籲、勸說員工為健康及防疫考量，自願安裝使用追蹤 App[190]。但如企業雇主當下發現，病毒因員工業務性質之故（例如在冷凍廠之封閉環境），可能在此特定工作場所中發生群聚感染現象，仍可以前述之理由要求員工安裝追蹤 App，但其中最重要的是，企業要求的指令必須內容明確，且經法律專家詳細檢視及作成紀錄，以免後續出現爭議。其中，企業還必須顧及勞動法對於員工各項權利的保障不得侵害，同時亦須徵詢工會意見，並取得其同意[191]。

在當員工安裝並開始使用追蹤 App 後，若因 App 發揮功能通報特定員工接觸過確診者，以致於進行居家隔離後，必須暫時離開其工作職務。企業雇主在呼籲、強制員工安裝使用追蹤 App，雖在防疫期間屬於不得不為之措施，惟一旦員工被通報疑似感染且須進入隔離，則企業雇主必須依據事先提出符合勞動法規之因應作法，也須承受可能的正反面後果。例如，企業員工是否有能力自行居家辦公或遠程處理公務，抑或缺少公共衛生官署依法發布之行政命令，以致員工接到企業的強制要求，仍然堅持不配合，而企業也不得予以懲處。再者，因員工在隔離期間不一定能全職遠端工作，所以薪資、

188 Rath/Feuerherdt (Fn. 18).
189 Rath/Feuerherdt (Fn. 18).
190 Schulzki-Haddouti (Fn. 187).
191 Deutscher Gewerkschaftsbund (Fn. 176); Rath/Feuerherdt (Fn. 18).

業績或整體績效計算也成為企業必須面對的問題，而此類問題並無法規或以往相關案例可茲依循[192]。

4.2　個資使用原則對員工安裝追蹤 App 義務之檢視

就企業於工作場域落實防疫措施的必要性而言，不論企業雇主與員工之間是否存在工作或買賣契約，各企業能否以雇主的身分強制員工基於公眾利益（保護健康）理由安裝追蹤 App，首先須從不同層次利益間之平衡與優先順序加以衡量[193]：

1.員工拒絕安裝追蹤 App 的利益：儘管安裝追蹤 App 對個資可能的侵害程度有限，但人民基於資料保護、共通之人格權及隱私權保護等權利拒絕安裝。

2.企業要求員工安裝追蹤 App 的利益：企業得依據德國《民法》第 611 條、第 241 條第二項、第 618 條及《工作者保護法》第 3 條、第 4 條規定，主張保護所有員工及顧客健康之權利，及維護自身營業利益的權利。

為檢視課予使用追蹤 App 義務是否符合歐盟《一般資料保護規則》第 5 條第一項[194]「處理之合法性」原則，必須針對上述兩種利益進行衡量，以確認當中比例原則的適用[195]。對此，必須檢視者，在於新開發的追蹤 App 對以下幾種利益的維護是否適當，首先，此一追蹤 App 是否確實能阻止員工從居住地出發至工作地點間，以及顧客於購物時的感染機率降低，並提高對該員工同事及其他周遭購物顧客不因接觸感染的保護程度。企業對於員工或許還因僱傭及職務關係而有相對之影響力，但顧客則無法強制要求，即使顧客進

192 Schulzki-Haddouti (Fn. 187); Rath/Feuerherdt (Fn. 18).

193 Deutscher Gewerkschaftsbund (Fn. 176); Schwenke (Fn. 10).

194 Art. 5 Abs. 1 DS-GVO.

195 MDR Sachsen, Darf der Chef den Download der Corona-Warn-App anordnen?, online verfügbar unter https://corona.betriebs-berater.com/1639/2020/darf-der-chef-den-download-der-corona-warn-app-anordnen-mdr-de/ (zuletzt geprüft am Dez. 16, 2022); Schwenke (Fn. 10).

入公司或店面時迅速安裝並出示給店員，表示已遵循購物場所規範，但離開後即可加以卸載不用，因此以立法強制推行是否有效，則不無疑問[196]。其次，在確保企業、員工及顧客利益的前提下，尚須考量是否有效果類似，但負面影響較為輕微之措施，例如引進配戴口罩義務、空間分隔、確保社交距離、居家辦公室及網路會議等，抑或是對特定職業從業人員之專業訓練，像醫護人員對病毒傳染途徑的教育課程，及企業或營業場所內部防疫流程的規律檢視等，不必直接使用個資或干預個人隱私領域之低度介入措施。假如前述輕微措施效果不彰，違規不遵守者多，則再大量投入追蹤 App 進行防疫，屆時大眾對安裝使用產生的疑慮就會降低[197]。

另需考量者還有使用追蹤 App 對企業員工個人人格權及隱私權造成的負擔，是否在可忍受的適當範圍內。通常資料保護及隱私領域在司法程序中，法官對其不應受限之價值判斷比重，常認為高於為使用追蹤 App 而限制人格權及隱私權之必要性，特別是這些對人權的限制是為了維護追蹤 App 的正面效用及成果評估。此種禁止就如同德國《刑法》原則所述之「不當連結之禁止」（in dubio pro libertate）及歐盟《一般資料保護規則》第 5 條第一項「目的性連結」[198]。另歐盟《一般資料保護規則》第 7 條第四項[199]亦有規定，當評估授權是否依當事人自由意願提出時，必須在最大可能的範圍，考量實際狀況及各種條件後加以判斷，包括提供勞務在內之契約履行要件，是否依據當事人對個資處理之自願授權而定，特別是授權同意處理個資於契約之履行並非必要時，則企業為保護個人健康，強制員工或顧客用追蹤 App 管控感染範圍，導致員工、顧客人格權及隱私權受到損害的措施，可能逾越比例原則，而被法院認定為違法無效。在大多數的案例，此一利益衡量過程儘管被公共衛生主管官署謹慎地執行，但仍導致適用上的模糊地帶[200]。

196 Deutscher Gewerkschaftsbund (Fn. 176).
197 Schwenke (Fn. 10).
198 Art. 5 Abs. 1 Buchst. b DS-GVO.
199 Art. 7 Abs. 4 DS-GVO.
200 Schwenke (Fn. 10).

因追蹤 App 並非企業自行研發，而係德國聯邦政府委外開發後，提供免費下載使用，故產業界有不同意見認為，企業是配合政府防疫政策推動，並不是追蹤 App 政策之制定與推動者，故依歐盟《一般資料保護規則》第 4 條第七款[201]規定推論，應由公共衛生主管機關及防疫機構「羅伯特科赫研究所」承擔個資法上之相關法律責任，而非各企業或民間組織。對此也有不同見解指出，企業雇主其實有很多不同的防疫科技工具或實體措施可以選擇，然而卻常常為了企業成本及便利計，直接採用一種雖符合歐盟《一般資料保護規則》第 25 條第一項[202]規定，但同時卻有違反德國《聯邦資料保護法》第 26 條第一項[203]，及歐盟《一般資料保護規則》第 6 條第一項第 f 款[204]所示必要性原則疑慮之科技工具，例如防疫用途的追蹤 App[205]。

企業此舉雖有模糊地帶的爭議，但藉此可在無須付出自行研發成本的前提下，無阻礙的要求所屬員工或接觸之外部人員必須採用追蹤 App。但因聯邦政府最終在反對壓力下，採用自由意願安裝之立法模式，以符合《聯邦資料保護法》及歐盟《一般資料保護規則》之規定，因此企業除非符合歐盟《一般資料保護規則》第 9 條所定之例外要件，否則不得強迫員工或顧客安裝追蹤 App。而企業員工及顧客之人格權、隱私權與防疫下大眾之健康權，均能處於立足點相同之位置，由法院予以衡量，不至於因立法強制使用並課予法定義務之故，而產生公眾健康利益似乎高於個人人格權與隱私權之謬誤[206]。

---

201 Art. 4 Nr. 7 DS-GVO.

202 Art. 25 Abs. 1 DS-GVO.

203 § 26 Abs. 1 BDSG.

204 Art. 6 Abs. 1 S. 1 Buchst. f DS-GVO.

205 Katharina Schmitt (Jun. 16, 2020), Was Arbeitgeber zum Einsatz der Corona-Warn-App wissen müssen, online verfügbar unter https://www.haufe.de/personal/arbeitsrecht/corona-warn-app-was-arbeitgeber-zum-einsatz-wissen-muessen_76_518650.html (zuletzt geprüft am Dez. 18, 2022).

206 Deutscher Gewerkschaftsbund (Fn. 176); Schwenke (Fn. 10).

4.3 從德國《聯邦資料保護法》規定判斷員工追蹤 App 安裝義務

關於雇主得否強制員工安裝並開啟追蹤 App 的法源依據，除了歐盟層級《一般資料保護規則》給予之共同規範外，在國內法層面，還可從德國《聯邦資料保護法》第 22 條、第 23 條、第 26 條、第 28 條、第 32 條[207]之規定加以判斷。為符合歐盟《一般資料保護規則》立法後之新標準，各國立法者均開始透過修法或立法，納入歐盟保護個資之各類要件，以免牴觸歐盟《一般資料保護規則》。同時，在歐盟《一般資料保護規則》賦予各成員國訂定符合國內需要之授權規定下，德國國會就現行《聯邦資料保護法》中之規定，亦有增修必要之規定。其中，《聯邦資料保護法》第 22 條第一項[208]規定，雖與歐盟《一般資料保護規則》第 9 條第一項[209]規定有違，但在符合該條規範意旨之情況下，仍為允許。第 22 條第一項第一款[210]即規定，當符合以下要件時，得允許公部門（例如防疫主管官署）或非公部門（例如企業及醫療院所）對個人特種個資之處理：

1.當處理特種個資係為執行落實社會安全、社會保護權利之法律，以及履行其伴隨之義務所必要者（第一款第 a 目）；

2.為衛生預防之目的、員工工作能力之評估、醫學診斷、衛生及社會相關照護與處理、衛生及社會事務機構與工作人員之行政，抑或基於相關人與衛生職業所屬人員間之企業有必要，以此等個資由醫療人員或由其他負有相關保護義務或責任者加以處理（第一款第 b 目）；

3.在公共衛生領域內因公眾利益的的理由，如嚴重跨邊境健康危害之防護，或為保障健康照護、醫師處方藥品及醫療用品生產之高度品質與安全標準有必要者（第一款第 c 目前段）；

---

207 §§ 22, 23, 26, 28, 32 BDSG.

208 § 22 Abs. 1 BDSG.

209 Art. 9 Abs. 1 DS-GVO.

210 § 22 Abs. 1 Nr. 1 BDSG.

4.因明顯公眾利益理由而有強制之必要者（第一款第 d 目）。

由以上《聯邦資料保護法》第 22 條規定可知，雇主是否可強制要求員工安裝追蹤 App 的前提，除了必須在勞雇關係存續中之必要行為外，在符合維護社會安全、公眾健康、醫藥研發、醫療照護及防治傳染病擴散等法律列舉要件，以及在其他明顯公共利益需要下，特別是新冠病毒變種株持續造成難以有效阻止之第三、第四波大規模群聚感染，對公共健康利益顯有高度危險，在疫苗接種率尚屬偏低時，強制員工在值勤時間開啟安裝追蹤 App 的公務用行動電話或載具，避免與客戶接觸或員工在工作場域接觸感染，應符合保護公眾健康利益的目的[211]。但由此可知，屬員工個人使用之行動電話及載具，其儲存之資料多為個人隱私之圖文、影音或照片，與公務無關，雇主自不得要求員工安裝。

至於公部門，特別是防疫主管官署，在防疫期間若要以科技防疫工具，或各類防疫科技執行防疫措施，均有可能違反個資蒐集與處理之既有目的，且祇範圍與程度高於私人企業。對此，有別於《聯邦資料保護法》第 22 條第一項第一款[212]公、私部門同時適用於例外狀況之阻卻違法要件，在同項第二款則另就公部門，特別是在防疫期間，防疫主管官署處理特種個資之例外情況，列舉以下之法律要件：

1.為避免公共安全遭受明顯之危險而有必要者（第二款第 a 目）；

2.為避免公共福祉益遭受明顯之不利而有必要者（第二款第 b 目），或為強制保障公共福祉之明顯利益而有必要者（第二款第 c 目）；

3.基於防衛或履行聯邦機關國家間義務之強制理由，在消除危機或阻止衝突範圍內採行人道措施之必要者（第二款第 c 目）。

至於第一項第一款第 d 目及第二款關於負責人員（Verantwortlichte）處理特種個資之利益，必須高於個資相關人本身之利益。另，《聯邦資料保護法》第 22 條第二項規定，則針對第一項特種個資處理情況，課予負責人員採

211 Deutscher Gewerkschaftsbund (Fn. 176); Connect.de (Fn. 15).

212 § 22 Abs. 1 Nr. 1 BDSG.

取適當及特定導護措施，維護個資相關人利益之義務。同時，本項亦要求個資處理之負責人員，經考量現實技術發展狀態、執行資料處理成本、執行方式、影響範圍，並評估可能造成自然人自由權利損害風險之機率，以及傷害之嚴重程度後，應採取符合歐盟《一般資料保護規則》第 25 條第一項[213]「隱私預設」（Privacy by Design）要求之保護措施。

追蹤 App 對特種個資之使用，既然係由用戶自願同意後下載，所以追蹤 App 傳輸、儲存及處理個資有其特定目的及授權範圍，防疫主管官署在蒐集、傳輸與處理個資之時，不得變更授權目的或逾越授權範圍。對此，歐盟《一般資料保護規則》第 6 條第一項第 c、e 款分別規定[214]，依法處理個資除相關人自願事先授權外，若係為履行法定義務而有必要，且負責人員承擔此法定義務者，則得以違反當事人或相關人員先授權同意之目的，處理其個資；個資處理係為保護相關人等同生命價值之利益，或其他自然人所必要者；若個資處理係負責人員為完成公眾利益之任務，以及執行公權力所必要者，則視為依法處理，例如防疫 App 蒐集之行動個資具有匡列確診者行動軌跡之可行性，且有保護公眾健康利益之實際效果，故防疫主管官署為保護公眾健康利益，則可依據前述規定。

儘管前述規定允許公部門基於公眾健康等重大利益，處理資料時可逾越原蒐集個資目的或範圍，但同時在同條第三項第一款也有限制性之規定，以免公部門之負責人員以公眾利益為理由，濫用行政裁量權限。換句話說，負責人員依歐盟《一般資料保護規則》第 6 條第一項第 c、e 款處理個資，必須有歐盟法或會員國國內法課予之法定義務，且不得違反各該法律保護個資之規定。歐盟會員國防疫主管官署之負責人員或防疫人員，因公眾利益需要處理個資時，雖不符當初蒐集之目的，且未取得相關人對新使用目的之授權，但若該會員國之國內法允許此類違反既定蒐集目的執行之資料處理，則得依國內法規定視為合法之處理行為。所以國內法若明文規定於特殊情況下，得

213 Art. 25 Abs. 1 DS-GVO.

214 Art. 6 Abs. 1 Buchst. c, e DS-GVO.

不經相關人再次同意即可進行目的外使用，則優先適用此國內法之規定。

在以歐盟《一般資料保護規則》第 6 條賦予國內法作為逾越既有蒐集個資目的前提下，德國《聯邦資料保護法》第 23 條[215]另就公部門對不符個資蒐集目的之使用，列舉不同之法律要件。其中，第 23 條第一項[216]規定，公部門（例如聯邦衛生部）人員若係為執行其法定職務，得逾越既定個資蒐集目的，立即處理必要之個資，其要件列舉在以下各款[217]：

1.個資之處理明顯係為維護相關人之利益，且並無任何理由顯示，相關人知悉個資處理違反既有蒐集目的會拒絕其授權（第一款）；

2.當有事實上之跡象顯示，違反既有蒐集目的之個資處理並不正確，則公部門必須再次檢視個資相關人對其資料陳述之內容（第二款）；

3.個資處理為避免公共福祉益遭受明顯不利、公共安全遭到危害，或為了防衛國家安全、保障公共福祉等重要公益，及確保稅收和海關擔保而有必要者（第三款）；

4.個資處理係為保障他人權利免遭嚴重損害，而有必要進行者（第五款）。

此外，德國《聯邦資料保護法》第 23 條第二項[218]則就特種個資之處理，另有要求，此等資料之處理在歐盟《一般資料保護規則》第 9 條第一項規定之限制下，若要用於既有蒐集目的以外之處理，則必須符合該條第一項之條件與第二項[219]所列舉之阻卻違法要件，或者是德國《聯邦資料保護法》第 22 條[220]所規定之條件。

若雇主在勞雇關係存續中，欲強制要求員工安裝、使用防疫 App，則除

215 § 23 BDSG.
216 § 23 Abs. 1 BDSG.
217 § 23 Abs. 1 S. 1 bis S. 3, S. 5 BDSG.
218 § 23 Abs. 2 BDSG.
219 Art. 9 Abs. 1 bis 2 DS-GVO.
220 § 22 BDSG.

須不違反歐盟《一般資料保護規則》第 6 條、第 7 條、第 9 條[221]及其第 26 點[222]立法衡量理由外，尚須符合德國《聯邦資料保護法》之規定。對此，德國《聯邦資料保護法》第 26 條第一項前段[223]即有更詳細之規定，受僱員工之個人資料可於僱傭關係目的下加以處理，但必須是為了確定雙方僱傭關係是否建立，或於僱傭關係中，為履行或結束此一僱傭關係之義務，以及為了主張及履行由法律規定、薪資合約記載，或從工作內容協議推論出之員工權利與義務所必要者。其次，在同條第三項則規定，特種個資在歐盟《一般資料保護規則》第 9 條第一項[224]規定之限制下，若要用於原蒐集目的外之處理，則必須符合第 9 條第一項列舉之條件、第二項[225]之阻卻違法要件，亦不得違反德國《聯邦資料保護法》第 22 條[226]之規定。由此可知，若安裝追蹤 App 使用個資，係為履行法律保護勞工職業安全、身體健康及預防職業災害之義務，或強制安裝可從訂於勞動契約、工作協議等文件內之條款推論，係為維護僱傭關係（例如保護員工不致於因染疫而停職或離職）所採取之必要措施，則應可認為雇主可要求勞工在公務用行動電話或載具上安裝追蹤 App。

除一般個資外，追蹤 App 既然能比對確診者資訊，所以也會蒐集、傳輸及處理醫療相關之特種個資，對此《聯邦資料保護法》第 26 條第三項第一句[227]針對歐盟《一般資料保護規則》第 9 條第一項[228]規定之特種個資也設有例外條款。其規定，若在勞資僱傭關係中使用特種個資係為履行勞動法保護勞工權益、維持社會安全，或其他法定義務所必要者，且於當下並無實際證據顯示，相關人利益保護之價值優於特種個資在前述目的下的使用，故追蹤

221 Art. 6, 7 und 9 Abs. 1 DS-GVO.
222 Erwägungsgrund 26 der DS-GVO.
223 § 26 Abs. 1 S. 1 BDSG.
224 Art. 9 Abs. 1 DS-GVO.
225 Art. 9 Abs. 1 bis 2 DS-GVO.
226 § 22 BDSG.
227 § 26 Abs. 3 S. 1 BDSG.
228 Art. 9 Abs. 1 DS-GVO.

App 本身或 App 系統負責人員可依據例外條款，處理特種個資。

4.4　員工安裝 App 在公務與隱私領域的區別

在公務用之行動裝置是否可以強制要求安裝追蹤 App 方面，基本上可從私人用及公務用行動電話（裝置）兩大方向加以區別，企業雇主對員工私人領域的介入或其個人使用終端設備的干預相當有限，僅有在不得已之必要範圍內，才能要求員工在私領域的行為須配合企業政策。但是，由企業配發給員工使用之公務用（或公用）行動電話或各類行動裝置，因多為公務或商務使用，故受到之限制相對較低。兩者間之差異與判斷標準說明如下[229]：

4.4.1　安裝在私人行動電話或行動裝置

依自由意願決定是否安裝在私人行動電話或裝置，在 App 運作中，員工個人雖然在休假或非勤務中，但仍然受到追蹤 App 的監控，若此追蹤 App 在該員工之同事或其他社交圈內之安裝比例高，則此人的接觸者、接觸範圍及接觸對象（對方也有裝追蹤 App）之行動資料，都會以「匿名化」（Anonymisierung）之儲存格式，將去識別化後之數據資料，傳輸至防疫機構設立之中央伺服器或資料中心[230]。

4.4.2　安裝在公務用行動電話或行動裝置

若追蹤 App 係安裝於公務用行動電話或裝置，則 App 的人員接觸監控功能僅限於工作時間或業務相關期間，所以公務用行動裝置安裝追蹤 App 後，僅會介入公務層面及公務接觸人員，所以涉及個資之足跡追蹤辨識亦只與執行公務之人、事、時、地有關，對個人人格權及隱私權侵害之範圍與程度相對較輕[231]。此一初步分級方式，並非針對追蹤 App 使用義務是否合法或是否應立法規定，而係從公務及私人行動裝置，抑或各類安裝載具的角度來

229 MDR Sachsen (Fn. 195); Schwenke (Fn. 10).
230 Schwenke (Fn. 10).
231 Deutscher Gewerkschaftsbund (Fn. 176).

區別賦予義務的必要性。由於聯邦政府讓民眾依其自願安裝追蹤 App，並未賦予強制安裝之法定義務，所以社會大眾對於私人領域之行動裝置，因執行追蹤 App 而蒐集、傳輸及處理之個資是否會被防疫主管官署轉介其他資料庫，或於日後作為大數據進行分析，或用於公共衛生相關研究而感到疑慮，故自願同意下載之比例偏低[232]。儘管企業員工之公務用行動裝置在執行公務期間，企業可與員工約定安裝以保障工作場域內之員工或顧客之健康，但因無特別法明文授權企業強制員工安裝之法源，所以員工在非必要情況下，實際依照防疫需求而自願安裝於公務用行動裝置者亦不如預期。但因公務用行動裝置安裝追蹤 App 後，干預私人生活之程度，比安裝在私人行動裝置中的情況還低，所以一般民眾在公務用行動裝置上安裝追蹤 App 並於公務時段開啟使用的意願相對較高，對降低職場上群聚接觸感染的機率，仍有正面的助益[233]。

再者，從公民與國家之關係而言，追蹤 App 的使用是自願且事先授權，並無法律強制安裝義務，在企業與員工僱傭關係存續中，儘管外界有倡議認為應修改《傳染病防制法》之規定，授權雇主強制員工安裝追蹤 App 的法源，但目前聯邦眾議院尚未修法[234]。但若依照德國《民法》債篇所規定雇主與員工間之債法關係而觀，則目前產生的最大爭點在於雇主可否依據德國《營業法》（GewO）第 106 條[235]規定之「指示權」（Direktionsrecht），命令員工安裝並使用追蹤 App[236]。就目前對《營業法》第 106 條[237]之見解認為，對於執勤所使用之企業配發公務手機或載具，雇主可以「指示權」命令

232 Schmitt (Fn. 205).

233 Schwenke (Fn. 10).

234 Fuhlrott (Fn. 184), S. 275.

235 § 106 GewO.

236 Katja Giese (Jun. 17, 2020), Die Corona-App: Ein Muss oder Kann im Arbeitsverhältnis?, Kliemt Arbeitsrecht, online verfügbar unter https://www.lexology.com/library/detail.aspx?g=7f724251-d586-423f-8ac9-4b280fca759d (zuletzt geprüft am Aug. 20, 2021); Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

237 § 106 GewO.

員工安裝並使用追蹤 App，但對於員工在私領域範圍內使用之個人所有載具、手機或相關物品，雇主並無命令安裝追蹤 App 的「指示權」，與此相對之狀況者，則是公務用手機及載具，雇主必須說明此手機或載具確實由雇主提供員工作為公務使用，則有「指示權」之適用[238]。

儘管有見解認為雇主可以「指示權」命令員工在公務手機上安裝追蹤 App，但此舉無疑與推動 App 使用之自願事先同意原則有違，對此也產生不同立場之意見與爭議。其中，特別是企業雇主即便得依據《聯邦資料保護法》第 26 條[239]規定之介入規範（datenschutzrechtliche Eingriffsnormen）合法處理個人資料，但雇主仍不得以此作為隨意處理員工個資之理由。但若依據歐盟《一般資料保護規則》第 88 條第一項及《聯邦資料保護法》第 26 條第一項[240]之規定，對於企業雇主在僱傭關係中針對業務執行必要所蒐集、處理之員工個人資料，則並未受到限制。其中，也包括依據《聯邦資料保護法》第 26 條第三項[241]規定所保護之員工個人醫療及健康資料。「聯邦勞動法院」（Bundesarbeitsgericht）則多次透過判決見解指出，員工個人醫療與健康資料具有高度保護價值，不能無故或隨意透過「指示權」加以干預[242]。就《聯邦資料保護法》第 26 條第四項[243]規定而言，不同見解認為基於個人資料之高度保護價值，員工自可拒絕企業經營階層的指示權限，而企業經營階層與員工間或工會間的協議，亦不能當作處理或利用員工個人資料之合法授權[244]。至於在值勤以外的下班時間或休假期間，企業經營階層管理權限或命

238 Giese (Fn. 236) ; Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

239 Art. 88 Abs. 1 DS-GVO; § 26 BDSG.

240 Art. 88 Abs. 1 DS-GVO; § 26 Abs. 1 BDSG.

241 Art. 88 Abs. 1 DS-GVO; § 26 Abs. 3 BDSG.

242 BAG, NZA-RR 2019, S. 475; Axel Bertram, Zum Auskunftsanspruch des Betriebsrats über sensible Arbeitnehmerdaten, GWR 2019, S. 450; Fuhlrott (Fn. 184), S. 275.

243 § 26 Abs. 4 BDSG.

244 BAG, NJW 1971, S. 162; Christian Arnold, in: Kiel/Lunk/Oetker (Hrsg.), Münchener Handbuch zum Arbeitsrecht, 4. Aufl., 2018, § 315 Rn. 60.

令權限，並不適用，且企業內部既有規則亦須排除[245]。進一步來說，企業雇主在工作期間以命令要求員工安裝、使用追蹤 App，則與前述「聯邦勞動法院」之判決見解有違，因為雇主此一命令權明顯違反德國《企業組織法》（Betriebsverfassungsgesetz）第 75 條[246]規定，是為對員工隱私違反比例原則的過度介入，而且員工之隱私權本為企業經營者在勞雇關係中應保障之勞工基本權利[247]。

目前德國多個邦層級法院對於聯邦政府或邦政府的實體防疫措施，已有相關判決支持行政機關的作為。但對於追蹤 App 使用之爭議，則邦法院尚無直接判決可茲依據[248]。雖然追蹤 App 之安裝推廣政策，以及在個人同意下，個資與中央伺服器之連結都在合法範圍內，然使用中並非沒有因灰色地帶而產生的爭論，但法院之所以尚無直接判決或相關見解，主要仍受到新冠病毒擴散尚難以全面控制，導致政治與社會趨勢的改變，以及改變後的狀態對法院的影響有關[249]。但亦因安裝使用追蹤 App 並非法定義務，所以對員工或顧客的強制要求不合法，致使民眾自願安裝、使用的比例偏低。當追蹤 App 使用者過低時，其運作之效果也會連帶降低，因為用戶數太少，導致系統無法透過中央伺服器比對同樣有安裝者之識別訊號，即便確診者在附近，有近距離接觸感染的風險，追蹤 App 也不會發出警示，用戶自無法於獲知後，立即離開當地或返家進行隔離。甚至還可能因未收到警示訊息，以為周遭無感染者而放鬆防備（例如脫下口罩、未保持適當社交距離等），徒增感染機率[250]。

---

245 BAG, NJW 1971, S. 162; Arnold (Fn. 244).

246 § 75 BetrVG.

247 BAG, BAG, 21.02.2017 - 1 AZR 292/15: Altersgrenzenregelung in Betriebsvereinbarung, NZA 11, 738 (2017); BAG, BAG , 12.12.2006 - 1 AZR 96/06: Regelungskompetenz der Betriebsparteien, NZA 8, 453 (2007); Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

248 Schmitt (Fn. 205); Schwenke (Fn. 10).

249 Schmitt (Fn. 205); Schwenke (Fn. 10).

250 Deutscher Gewerkschaftsbund (Fn. 176); Schwenke (Fn. 10).

立法者讓民眾自行決定安裝與否，表示在無法律義務要求下，個人若不願意安裝，原則上是不得強制其下載使用。但同時法律並未將「自願」列為安裝 App 的免責要件，無疑是將責任轉嫁給民眾，由民眾自行承擔決定安裝與否的結果[251]。由此可知，若個人具有特定企業員工身分，且企業層主動要求員工安裝，雖然在非緊急狀態下員工可加以拒絕，但若因員工不願意安裝追蹤 App 導致可能因接觸感染者而必須居家隔離，甚至因受到感染而必須住院治療，則不排除因後續隔離、治療無法工作的時間，可能減少員工薪資收入，影響生活水平，抑或造成企業損失而致解僱或停班等勞資糾紛，而「自願」既非法定要件，則處於相對弱勢的員工是否能據此保障自身權益，不無疑問[252]。

4.5　公務手機追蹤 App 發出警示之雇主通報義務

如果追蹤 App 發出警示或顯示感染風險狀態時，則使用 App 的員工除了必須通報防疫主管機關外，是否有義務同時通報其企業雇主，仍有爭議。若先考量防疫 App 必須由員工自願之事前同意下載使用，以及員工個人醫療資料保障之利益等前提，則通知雇主的義務似乎與保障員工敏感個資之目的衝突，但員工與雇主之間仍存有勞務契約之債法關係，因此通報義務亦可視為德國《民法》第 241 條第二項規定之附屬義務[253]。另就德國《工作者保護法》（Arbeitsschutzgesetz）第 3 條第一項、第 9 條第二項，以及《民法》第 618 條規定[254]可知，雇主藉由獲得適當之訊息，可採取適當之保護措施，預防其他員工遭到感染。但相同的，為了保護員工所採取的相關措施也如前述向雇主通報之義務，也可視為附屬義務之一部分。不論是員工個人資料或雇主基於勞動企業保護員工安全之義務，均受到法律保障，因此若要判斷雇主是否得以要求員工安裝防疫 App，除了員工使用的載具或手機是否公務用之

251 Deutscher Gewerkschaftsbund (Fn. 176); Schwenke (Fn. 10).
252 MDR Sachsen (Fn. 195); Schwenke (Fn. 10).
253 § 241 II BGB.
254 §§ 3 I, 9 II ArbSchG; § 618 BGB.

外，尚須從員工個人與第三人（其他員工或不特定之接觸者）之法益加以衡量，而其中必須考量者還包括保障員工一般個資或健康醫療個資安全，與第三人可能遭受感染風險及健康損害之間比例權重。儘管對於利益衡量有許多爭議，但不同立場的見解多肯定，雇主對於員工身體狀態應有詢問義務[255]。另外，有見解持正面意見認為，雇主要求員工回報身體健康狀態只限於保護其他員工身體健康的情況，而且相關措施必須符合維護員工整體健康的目標，且禁止雇主以個人理由辭退為威脅手段，強迫員工告知健康狀態、強迫回報採檢結果及安裝追蹤 App[256]。

當員工從手機接到追蹤 App 發出的風險與警示訊號後，表示可能在近距離接觸確診者，故有相當大的感染風險。面對可能的感染風險，員工理應通報防疫官署並採取相關隔離措施，但問題是，員工能否因隔離的必要，而同時自行向主管機關通報處於「無執行工作能力」（Arbeitsunfähigkeit）之狀態，並向雇主要求帶薪停職。「聯邦醫師公會」（Bundesärztekammer）認為，依據德國《工資續付法》（Entgeltfortzahlungsgesetz）第 3 條規定[257]，員工應於接到追蹤 App 發送之警示，並向主管機關通報後，才會因隔離檢疫無法執行工作職務，故非直接感染病毒而失去工作能力，因此雇主不能就此認為該員工已無工作能力，而加以停薪停職[258]。實際上，員工收到警示訊息時，若無任何發病症狀，或隔離時亦無症狀，或核酸檢定亦為陰性，則並不符合法律定義之無工作能力或失去工作能力。但因考量新冠病毒的高傳染性，以及接觸者可能造成病毒大量擴散的風險，所以員工於隔離期間，應可透過遠距上班模式（Home Office）代替正常上班模式，以減少接觸感染機

255 Volker Stück/Boris Wein, Pandemie und Arbeitsrecht. Welche Vorkehrungen können Unternehmen treffen?, AuA 2020, S. 200 (200-206); Michael Fuhlrott, Arbeitsrechtliche Fragestellungen im Zusammenhang der Coronavirus-Epidemie, GWR 2020, S. 107 (107-110).

256 Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

257 § 3 EFZG.

258 Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

率。但若是雇主接到防疫主管機關之通知，並依據《工資續付法》第 3 條規定要求員工返家隔離，則該員工因隔離無法工作等同時失去工作能力，則雇主得單方面決定員工必須無薪停職[259]。

在此種情況下，雇主不需要在員工隔離或疑似染疫的情況下繼續支付薪資。儘管雇主有此權利，但仍應衡量勞資雙方僱傭契約關係中之義務及互信，此外還應徵詢企業特約醫師或直接於員工詳談後，才能決定該員工能否帶薪停職，或直接留職停薪。然而必須要注意的是，前述的狀況是以防疫主管機關通知雇主為前提，假若只是追蹤 App 發出接觸疑似確診者的警示，則一方面員工不得以此為理由要求帶薪停職，相對的，雇主也只有在員工被防疫主管機關依《傳染病防治法》第 56 條第一項[260]送特定地點隔離的情況下，才能主張其對員工要求返還隔離時停職已給付之薪資[261]。

值得注意的是，因員工在公務手機上安裝追蹤 App 關係勞工權益，因此雇主得出席工會代表會議表達意見。依德國《企業組織法》（Betriebsverfassungsgesetz）第 87 條第一項第一款對秩序行為（Ordnungsverhalten），及第 87 條第一項第七款對健康保護（Gesundheitsschutz）之規定，可推論出資方參與工會代表會議之權（Beteiligungsrechte der Arbeitnehmervertretung）[262]。因此雇主對使用追蹤 App 的建議，關係員工健康及職場公共衛生等事件，應可形成雇主（資方代表）出席工會代表會議權，但此一權利之前提在於勞資雙方在勞動契約協議上，即有將「流行病擴散」納入參與工會代表會議之要件[263]。

259 Fuhlrott (Fn. 184), S. 275.
260 § 56 I IfSG.
261 Fuhlrott (Fn. 255), S. 107-110.
262 § 87 I Nr. 1 BetrVG (Ordnungsverhalten) bzw. aus § 87 I Nr. 7 BetrVG (Gesundheitsschutz).
263 Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

5. 法制走向與結論

從德國聯邦政府研發追蹤 App 到上架推出，社會各界對此項政策是否適當，也有相當多不同立場意見。例如在 App 的風險評估中有反對意見認為，追蹤 App 推出時間僅數個月，其於防疫的實際成效還不明顯，雖不能說長期使用不會有阻擋病毒擴散的效果，但也有可能為了推動追蹤 App 而對相關基本人權的限制，最終仍徒勞無功，以致失去其限制的正當性與必要性。追蹤 App 是科技工具，因此不可能百分之百不會出現錯判或誤報警示的狀況，所以有許多狀況是需要預估並視實際狀況因應，然若追蹤 App 技術出現錯誤，並導致侵入個人隱私領域狀況不斷發生，個人或社會大眾對此一技術的信任與容忍將隨之下降[264]。

就像是 App 會偵測距離，但無法判斷當下的場域對用戶是否一定處於高感染風險的處境，而當民眾之間有玻璃片或圍牆隔絕，又或兩人位於上下樓層或兩個相鄰都不互通的房間，並沒有任何感染風險。但因行動電話或裝置的藍芽訊號可接收與感測到對方，所以可能也會視為近距離接觸並發動警示，並要求用戶居家隔離檢疫[265]。另外，當用戶在戶外、行車中，或將行動電話或裝置放在行李或衣物口袋中，都可能影響裝置的訊號強度，較弱的訊號亦無法偵測他人距離並回傳，反而真正接觸確診者之用戶因不知情而四處移動，進而讓感染擴大。如果防疫機構或地方行政機關也因接受 App 的誤判結果，而要求用戶隔離，導致該用戶行動受限，甚至損失薪資收入，無疑也是對用戶行動自由、工作權及財產權的侵害。用戶無故所受之經濟損失，尚無明確救濟辦法或法律依據[266]。

在防疫期間，App 等科技工具應用在阻擋疫情擴散有其較平常時期更高的必要性與急迫性，但若是在同樣需要限制部分行動自由權及資訊自決權的

264 Kötter (Fn. 7).
265 Stör (Fn. 23); Kötter (Fn. 7).
266 Kötter (Fn. 7).

情況下，則應採用健康保護效果類似，但對於個人隱私或人格權造成危害的風險相對較低的政策措施與科技方法。例如一般所知的保持 1.5 公尺社交距離、個人單獨辦公室、居家辦公、公共場所及搭乘大眾交通工具時配戴口罩，以及穿著防護衣等[267]。如果此類措施在特定領域、區域或場所範圍內落實之要求程度高，抑或在特殊例外狀況下難以由員工個人決定的情況下，例如為了老人、兒童、育幼或健康醫療場所等場域之工作者，則企業雇主對其員工，應可援引歐盟《一般資料保護規則》第 9 條[268]的例外條款規定，在合理範圍內，要求員工於公務用行動裝置內，安裝防疫用追蹤 App。但企業雇主僅可於執勤（公務）時間、公務相關工作場域，及其他使用公務用行動裝置執行公務的情況下，要求員工使用追蹤 App。除此之外，如員工處於休息、假日或下班時間，則企業雇主不得強制員工開啟安裝在公務用行動裝置的追蹤 App，或以防疫名義要求追蹤 App 的偵測狀態[269]。

以 App 科技工具控制感染範圍在技術層次自有高度可行性，但在法律層次上，因 App 使用大量「假名化」（Pseudonymisierung）之一般及敏感個資，在未經個人自願同意下，個資存在被數位平台蒐集並提供行政機關使用之潛在風險。反對者認為，個資使用未經同意係違反個人行動自由、隱私及資訊自決等重要權利，但支持者則認為，資料保護過度及實際應用過於保守，反而才會違反個人「健康完整無缺」的基本人權[270]。正反意見之間雖各有立論見解，但彼此對立並無共識。實際上，德國防疫機構以自願方式推動追蹤 App 等科技工具進行防疫，原則上並未違反歐盟《一般資料保護規則》、德國《全國範圍流行病情勢下之國民保護法》、《全國範圍流行病情勢下之國民保護法第二次法案》，以及《傳染病防治法》之既有規定，但從個人資料蒐集、儲存、傳輸與處理等後續作為衍伸出侵害基本人權與否的疑慮，以及該如何確保追蹤 App 之應用目的、對象及執行範圍不會被行政機關

267 Rath/Feuerherdt (Fn. 18).
268 Art. 9 DS-GVO.
269 Rath/Feuerherdt (Fn. 18).
270 Weiss/Strauß (Fn. 32); Kümmerle (Fn. 31).

無故擴張；大眾之個資受侵害時，有何救濟途徑等議題，則尚無法律明文保障，其漏洞亟待國會立法或修法予以補正。現階段大眾注目的焦點在防疫成效，因此對於防疫機構使用個資的容忍度較高，一旦疫情趨緩，不排除大眾將更嚴格檢視防疫期間科技工具是否濫用個資，或造成對基本人權的不當限制。不論是行政或立法機關皆須審慎思慮的是，科技工具就如同兩面刃，用於防疫可產生阻絕病毒感染擴散的效果，但同樣也會對人權造成不可回復的侵害，因此，如何平衡兩者不單是防疫機構或專業人士單方面的考量，更應是社會大眾應具備的意識。

基於目前多變的疫情狀態，以及德國全國疫情大流行狀態的持續進行中，因此哪些相對應的策略及作為，會對整體社會、經濟及公共衛生政策的執行產生不同程度的影響，以及哪些正反面之效果，可說已相當明顯，除了新冠疫苗的廣泛接種與積極推動外，仍然需要如同追蹤 App 等科技工具的協助，方能控制第三波或第四波由變種病毒株帶來的疫情。實際上，科技工具對個人基本權利的干預，相對於長期的出入限制、禁止集會、禁止餐飲營業、禁止休憩活動，甚至封城，可說是程度較輕的措施，在以個人自願事先授權為前提的情況下，可說是較能符合比例原則，並獲得人民信任及值得採用的防疫策略[271]。然而最重要的是，唯有當大眾對國家機關行政作為的警覺心愈高，人權受不當限制的風險才會愈低，法律對權利的保障也才能真的落實。

271 Achim Klabunde, in: Dahl/Göpfert/Helm (Hrsg.), Arbeitsrechtlicher Umgang mit Pandemien Praxisleitfaden am Beispiel der Corona-Krise, 2020, S. 153 f.; Fuhlrott (Fn. 184), S. 275; Köllmann (Fn. 184), S. 831.

參考文獻

德文書籍

Firg, René, Strukturelle Analyse des allgemeinen Persönlichkeitsrechts anhand des Rechts auf informationelle Selbstbestimmung, 2015, Hamburg: Dr. Kovač.

Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander, Informationelle Selbstbestimmung im digitalen Wandel, 2017, Wiesbaden: Springer Vieweg.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung, 2016, Tübingen: Mohr Siebeck.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, Tübingen: Mohr Siebeck.

德文期刊

Bertram, Axel, Zum Auskunftsanspruch des Betriebsrats über sensible Arbeitnehmerdaten, GWR 2019, S. 450.

Fuhlrott, Michael, Arbeitsrechtliche Fragestellungen im Zusammenhang der Coronavirus-Epidemie, GWR 2020, S. 107-110.

Fuhlrott, Michael, Corona-Warn-App: Nutzungspflicht für Arbeitnehmer?, GWR 2020, S. 275-277.

Köllmann, Thomas, Die Corona-Warn-App, NZA 2020, S. 831-836.

Samardzic, Darko/Becker, Thomas, Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW 2020, S. 646-653.

Stück, Volker/Wein, Boris, Pandemie und Arbeitsrecht. Welche Vorkehrungen können Unternehmen treffen?, AuA 2020, S. 200-206.

德文論文集

Klabunde, Achim, in: Dahl/Göpfert/Helm (Hrsg.), Arbeitsrechtlicher Umgang mit Pandemien Praxisleitfaden am Beispiel der Corona-Krise, 2020, Frankfurt am Main: Fachmedien Recht und Wirtschaft.

德文法律註釋及手冊

Arnold, Christian, in: Kiel/Lunk/Oetker (Hrsg.), Münchener Handbuch zum Arbeitsrecht, 4. Aufl., 2018, München: C. H. Beck, Art. 315.

Buchner, Benedikt/Petri, Thomas, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG Kommentar, 2. Aufl., 2018, München: C. H. Beck, Art. 6.

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried, in: Gierschmann (Hrsg.), Kommentar DS-GVO, 2018, Köln: Reguvis, Art. 6.

Hladjk, Jörg, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, München: C. H. Beck, Art. 22.

Klabunde, Achim, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, München: C. H. Beck, Art. 4.

Schiff, Alexander, in: Ehmann/Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., 2018, München: C. H. Beck, Art. 9.

Schreiber, Lutz, in: Plath (Hrsg.), DSGVO/BDSG Kommentar, 3. Aufl., 2018, Köln: Dr. Otto Schmidt, Art. 4.

Schulz, Sebastian, in: Gola (Hrsg.), Datenschutz-Grundverordnung (DS-GVO) Kommentar, 2. Aufl., 2018, München: C. H. Beck, Art. 6.

Wolff, Heinrich Amadeus, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar zu EUV, GRC und AEUV, Bd. II, 2017, Tübingen: Mohr Siebeck, Art. 8 GRC.

其他德文參考文獻

BNetzA (2020), Nutzung von OTT-Kommunikationsdiensten in Deutschland, Bericht 2020, Bundesnetzagentur, online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile (zuletzt geprüft am Apr. 3, 2021).

BRAK, BRAK: Handyortung der Kontaktpersonen Corona-Infizierter nur als Ultima Ratio, online verfügbar unter https://rsw.beck.de/aktuell/daily/meldung/detail/brak-handyortung-der-kontaktpersonen-corona-infizierter-nur-als-ultima-ratio (zuletzt geprüft am Dez. 18, 2022).

Brink, Stefan und Clarissa Henning (Apr. 3, 2020), Digitalisierung in der Corona-Falle: Warum freiwilliges Handy-Tracking nicht funktioniert, Netzpolitik.org, online verfügbar unter https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert/ (zuletzt geprüft am Dez. 18, 2022).

Bundesegierung, Corona Warn-App: Unterstützt uns im Kampf gegen Corona, Die Bundesregierung, online verfügbar unter https://www.bundesregierung.de/breg-de/themen/corona-warn-app (zuletzt geprüft am Aug. 9, 2020).

Bundesegierung, Corona-Warn-App: Die wichtigsten Fragen und Antworten, online verfügbar unter https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392 (zuletzt geprüft am Dez. 18, 2022).

Bundesrat, Entwurf eines Zweiten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite, online verfügbar unter https://www.bundesrat.de/SharedDocs/drucksachen/2020/0201-0300/246-20.pdf?__blob=publicationFile&v=1 (zuletzt geprüft am Dez. 18, 2022).

Connect.de, Zahlen-Schätzung zu Positiv-Fällen. Corona-Warn-App: So viele Infizierte haben sich gemeldet, online verfügbar unter https://www.connect.de/news/corona-warn-app-gemeldete-faelle-infizierte-positiv-zahlen-schaetzung-3200916.html (zuletzt geprüft am Aug. 5, 2020).

Datenschutz-Folgenabschätzung (DSFA) für eine Corona-App, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), online verfügbar unter https://www.fiff.de/presse/dsfa-corona-digiges.html (zuletzt geprüft am Aug. 10, 2020).

Datenschutz.org (Nov. 18, 2022), Verbot mit Erlaubnisvorbehalt im Datenschutzrecht, online verfügbar unter https://www.datenschutz.org/verbot-mit-erlaubnisvorbehalt/ (zuletzt geprüft am Dez. 18, 2022).

Dehmel, Susanne/Kenning, Peter/Wagner, Gert G./Liedtke, Christa/Micklitz, Hans W./Specht-Riemenschneider, Louisa (2020), Die Wirksamkeit der Corona-Warn-App wird sich nur im Praxistest zeigen, Sachverständigenrats für Verbraucherfragen, online verfügbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Fachinformationen/PolicyBrief_Corona_APP.pdf?__blob=publicationFile&v=2.

Deutscher Gewerkschaftsbund (Jun. 19, 2020), Corona-App und Arbeitsrecht: Was darf mein Chef, Deutscher Gewerkschaftsbund (DGB), online verfügbar unter https://www.dgb.de/themen/++co++958547b4-b236-11ea-a4c5-52540088cada (zuletzt geprüft am Aug. 19, 2020).

Dörner, Karolin (Jul. 17, 2020), Corona-App: Wissenschaftler Kritisieren Rolle von Google und Apple, MDR Missen, online verfügbar unter https://www.mdr.de/wissen/Corona-warn-app-einschaetzung-leopoldina100.html (zuletzt geprüft am Aug. 2, 2020).

Giese, Katja (Jun. 17, 2020), Die Corona-App: Ein Muss oder Kann im Arbeitsverhältnis?, Kliemt Arbeitsrecht, online verfügbar unter https://www.lexology.com/library/detail.aspx?g=7f724251-d586-423f-8ac9-4b280fca759d (zuletzt geprüft am Aug. 20, 2021).

Greis, Friedhelm (Mai 28, 2020), FAQ zur Corona-App der Bundesregierung, Golem.de, online verfügbar unter https://www.golem.de/news/faq-was-man-ueber-corona-app-der-regierung-wissen-muss-2005-148749.html (zuletzt geprüft am Jun. 1, 2020).

Infektionsketten digital unterbrechen mit der Corona-Warn-App, Robert Koch Institut, online verfügbar unter https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (zuletzt geprüft am Dez. 18. 2022).

Kötter, Nicolas (Jun. 18, 2020), Die Corona-Warn-App – Fluch oder Segen?, Dr. Datenschutz, online verfügbar unter https://www.dr-datenschutz.de/die-corona-warn-app-fluch-oder-segen/ (zuletzt geprüft am Aug. 8, 2020).

Kümmerle, Madeleine (Mär. 3, 2022), Wichtige Datenschutzgrundsätze für die Verarbeitung von Daten, Dr. Datenschutz, online verfügbar unter https://www.dr-datenschutz.de/dsgvo-grundsaetze-fuer-die-verarbeitung-personenbezogener-daten/ (zuletzt geprüft am Dez. 18, 2022).

Leitlinien zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie, Europäische Kommission, online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN (zuletzt geprüft am Mär. 29, 2021).

Majcen, Patrick (Apr. 26, 2018), Praxishilfe Datenschutz: Wie lange darf ich personenbezogene Daten speichern?, Ikonline, online verfügbar unter https://www.lko.at/praxishilfe-datenschutz-wie-lange-darf-ich-personenbezogene-daten-speichern+2400+2704442 (zuletzt geprüft am Okt. 19, 2021).

MDR Sachsen, Darf der Chef den Download der Corona-Warn-App anordnen?, online verfügbar unter https://corona.betriebs-berater.com/1639/2020/darf-der-chef-den-download-der-corona-warn-app-anordnen-mdr-de/ (zuletzt geprüft am Dez. 16, 2022).

Pettinger, Bianca (Mai 14, 2020), Zweites Pandemiegesetz: Kein Datenschutz für Gesunde, Dr. Datenschutz, online verfügbar unter https://www.datenschutzbeauftragter-info.de/zweites-pandemiegesetz-kein-datenschutz-fuer-gesunde/ (zuletzt geprüft am Mai 17, 2020).

Rath, Michael/Feuerherdt, Gerrit (Mär. 11, 2021), Corona-App, DSGVO und Co. Datenschutz in der COVID-19-Krise, Computerwoche, online verfügbar unter https://www.computerwoche.de/a/datenschutz-in-der-covid-19-krise,3548738 (zuletzt geprüft am Dez. 18, 2022).

Rötzer, Florian (Mai 13, 2020), Datenerfassung von Gesunden: Lambrecht gegen Kelber, Heise Online, online verfügbar unter https://www.heise.de/tp/features/Datenerfassung-von-Gesunden-Lambrecht-gegen-Kelber-4719716.html (zuletzt geprüft am Mai 17, 2020).

Schaar, Peter (Mär. 30, 2020), Peter Schaar: Mit heißer Nadel gegen das Virus?, Heise Online, online verfügbar unter https://www.heise.de/newsticker/meldung/Peter-Schaar-Mit-heisser-Nadel-gegen-das-Virus-4693535.html (zuletzt geprüft am Mai 17, 2020).

Schmitt, Katharina (Jun. 16, 2020), Was Arbeitgeber zum Einsatz der Corona-Warn-App wissen müssen, online verfügbar unter https://www.haufe.de/personal/arbeitsrecht/corona-warn-app-was-arbeitgeber-zum-einsatz-wissen-muessen_76_518650.html (zuletzt geprüft am Dez. 18, 2022).

Schulzki-Haddouti, Christiane (Nov. 3, 2020), Medizinische Hochschule Hannover und Ubilabs entwickeln Corona-App, Heise Online, online verfügbar unter https://www.heise.de/newsticker/meldung/Medizinische-Hochschule-Hannover-und-Ubilabs-entwickeln-Corona-App-4680487.html?seite=all (zuletzt geprüft am Jun. 1, 2020).

Schwenke, Thomas (Jun. 17, 2020), Corona-Warn-App als Pflicht für Mitarbeiter und Kunden (FAQ und Praxistipps)?, Datenschutz-Generator, online verfügbar unter https://datenschutz-generator.de/corona-warn-app-pflicht-nutzung/ (zuletzt geprüft am Aug. 10, 2020).

Stör, Christian (Mär. 31, 2020), Corona-Virenschutz: Handy-Daten nutzen oder nicht - ist die App die Lösung?, Frankfurter Rundschau, online verfügbar unter https://www.fr.de/meinung/corona-virenschutz-handy-daten-nutzen-app-loesung-13634597.html (zuletzt geprüft am Mai 20, 2020).

Weiss, Maike/Strauß, Kathrin (Apr. 6, 2020), Corona und Datenschutz: Wie Handyortung im Kampf gegen das Virus helfen soll, Datenschutzexperte.de, online verfügbar unter https://www.datenschutzexperte.de/blog/datenschutz-im-alltag/corona-und-datenschutz-wie-handyortung-im-kampf-gegen-das-virus-helfen-soll/ (zuletzt geprüft am Mai 17, 2020).

Westenthanner, Marianne/Humpa, Michael (Jul. 21, 2020), Die Corona App – Risiken und Nebenwirkungen, Chip 365, online verfügbar unter https://www.chip.de/news/Corona-Warn-App-So-sieht-sie-aus-das-kann-sie_182639402.html (zuletzt geprüft am Aug. 12, 2020).

Wissenschaftliche Dienste (2020), Einzelfragen zum Handy-Tracking in Deutschland im Zusammenhang mit der Corona-Pandemie – Ausarbeitung, Deutscher Bundestag, online verfügbar unter https://www.bundestag.de/resource/blob/692998/c88738c96c087f66748ac75a0a7788b2/WD-3-098-20-pdf-data.pdf (zuletzt geprüft am Mär. 29, 2021).