COURT OF APPEALS OF VIRGINIA

PUBLISHED

Present: Judges Fulton, Lorish and White
Argued at Norfolk, Virginia

MATTHEW KEIL

v. Record No. 1621-23-1

JIM O'SULLIVAN, IN HIS OFFICIAL CAPACITY AS SHERIFF OF THE CITY OF CHESAPEAKE, VIRGINIA

OPINION BY
JUDGE LISA M. LORISH
AUGUST 27, 2024

FROM THE CIRCUIT COURT OF THE CITY OF CHESAPEAKE
William S. Moore, Jr., Judge Designate

Kevin E. Martingayle (Bartlett Keil; Bischoff Martingayle, PC; Green Hampton & Kelly, PLLC, on briefs), for appellant.

Jeff W. Rosen (Lisa Ehrich; Pender & Coward, on brief), for appellee.

Officer Matthew Keil requested information from his employer, the Chesapeake Sheriff's Office (CSO), related to an internal investigation the CSO undertook into Keil's conduct. He sent the requests under the Virginia Freedom of Information Act ("VFOIA"), §§ 2.2-3700 to -3715, and the Government Data Collection and Dissemination Practices Act ("Data Act"), §§ 2.2-3800 to -3809. After the CSO failed to reply to his Data Act request and claimed an exemption to his VFOIA request, Keil filed an action in the Chesapeake Circuit Court challenging the CSO's refusal to give him access to the requested information. The circuit court dismissed the action, finding that Keil was not entitled to access the internal affairs file because he was not a "data subject" under the Data Act, and because the CSO did not violate VFOIA. We find no error in the dismissal.

BACKGROUND

Keil was a sergeant with the CSO when deputies under his supervision used force against an inmate at the Chesapeake City Jail in December 2022. Following the incident, the CSO demoted Keil to Senior Deputy Sheriff and the CSO's Internal Affairs Division began investigating the incident. Upon learning of the investigation, Keil sent several VFOIA and Data Act requests to Sheriff Jim O'Sullivan requesting information about the investigation.

The January 6 Request

On January 6, 2023, Keil's lawyer requested body camera footage, audio or video records, and any documentary evidence relating to the incident at the Chesapeake jail under the federal Freedom of Information Act. The letter asked the CSO to "limit [its] search of the [requested] items" to evidence "from December 13 to the present." On January 13, 2023, counsel for O'Sullivan responded that he was considering the original letter to be a VFOIA request and claimed an exemption under Code § 2.2-3706(B)(4) and (B)(9).[1] On January 17, Keil's counsel emailed O'Sullivan's lawyer, "please consider [the January 6th request] to also be a request pursuant to the Government Data Collection and Dissemination Practices Act." On January 20, Keil's counsel emailed O'Sullivan to reiterate that Keil's "prior requests for records" were being made under both VFOIA and the Data Act, and sought a confirmation and response from O'Sullivan, including asking that he state any claimed exemptions. On January 23, O'Sullivan's lawyer responded by attaching the original VFOIA response he sent on January 13.

The February 9 Request

On February 9, Keil made a new request, now seeking a copy of his "entire employment/personnel [sic] that the Sheriff and/or his office maintains on [him], including all

[1] Whether the requested items of information are exempted from disclosure under VFOIA is not the subject of this appeal.

sub-files and records covered by [the Data Act]." On February 10, O'Sullivan informed Keil that his personnel file would be available to Keil within days. Keil received the personnel file.

The March 9 Request

On March 9, 2023, Keil sent a letter to O'Sullivan entitled "Renewed and clarified request on behalf of Matt Keil pursuant to Code of Virginia §§ 2.2- 3700 et seq. and 2.2-3800 et seq." The letter explained that "one of [its] purposes . . . is to clarify the nature and scope of the prior and current requests for information that have been and are being made by and for Matt Keil." To this end, the letter asked O'Sullivan to consider the requests sent on January 6 and "the follow-up communications" to have been made under both VFOIA and the Data Act. The letter also stated that it "constitutes a renewal of the request for all of [the] information" sought on January 6. "[T]o avoid any confusion about the scope of what is requested," the letter clarified that Keil sought his entire employment/personnel file, "including all sub-files and records covered by [the Data Act]" and that Keil "has requested and continues to request a copy of all of the evidence, records, video, and information . . . that relates in any manner to and/or supports" Keil's demotion in December 2022. Indeed, the letter noted that the personnel file provided to Keil was "clearly incomplete" because it did not include information related to his demotion.

Finally, the letter requested "any additional responsive information that relates in any manner to Matt Keil's appeal of [the decision to demote him] and/or the denial of his appeal." On March 28, Keil sent a follow-up email to O'Sullivan asking him to confirm receipt of the March 9 letter and requesting a reply.

Litigation Begins

After failing to receive another response from O'Sullivan, Keil filed a complaint and a motion for judgment in the Chesapeake General District Court. Keil argued that Code

§ 2.2-3806(A)(3) gave him the right to inspect personal information about him that was contained in the investigation file and that O'Sullivan's failure to respond to the March 9, 2023 letter violated Keil's rights under VFOIA and the Data Act. Keil sought a writ of mandamus compelling O'Sullivan to provide Keil with all records that he requested, an injunction preventing future violations, reasonable costs and attorney fees, and any penalty appropriate under VFOIA and the Data Act. At trial on May 10, 2023, Keil reasserted his right to the internal investigation file and sought access to his employment evaluations from 2011 to 2018, which did not appear in the personnel file provided to Keil. O'Sullivan did not object to turning over the employment evaluations, noting that, to the extent they were not in his personnel file, "it's an oversight." On May 23, 2023, O'Sullivan produced the evaluations.

After the general district court ruled against him, Keil appealed to the Chesapeake Circuit Court seeking the same relief and making the same arguments. In the circuit court, Keil asserted his right to "all of the information that is part of [the] investigation" and "anything else that is something that could be considered personnel information, employment information"; in other words, "whatever they've got on [Keil]."

O'Sullivan testified that the internal affairs investigation file was not indexed under Keil's name, nor was it indexed under an employee number. The file also was not searchable by name or part of Keil's personnel file. Instead, the sheriff's office categorizes internal affairs investigations, including the investigation into Keil, by year, and then assigns each investigation a sequential number. Additionally, during his testimony, O'Sullivan acknowledged that the personnel file provided to Keil in February lacked certain evaluations of his performance, but that this was an "oversight on us," and that the records were eventually provided to him.

On cross-examination, defense counsel asked Keil about the investigation into his conduct, and in doing so, referenced details about the incident in December 2022. Keil objected

on the ground that disclosing those details violated the Data Act. O'Sullivan responded that he was "putting the case in context . . . . [I]f you file and say you want records, the Judge is entitled to know what the records are and how they arose." The court sustained the objection.

During argument, Keil asserted that the internal investigation file and Keil's employment records are subject to mandatory disclosure under the Data Act because he is a "data subject" under the Act, which entitles him to "personnel information and personal information." Keil also argued that the Sheriff provided no defense under the Data Act for his failure to produce investigatory materials, which means he waived any defenses he might have under the Act and that failing to timely provide all the evaluations that were in his personnel file violated both VFOIA and the Data Act. Finally, Keil asserted that O'Sullivan violated the Data Act by unlawfully disseminating information about the incident that led to the December 2022 investigation by discussing it in a pre-trial brief[2] and throughout the litigation.

O'Sullivan contended that Keil was not entitled to receive information from the investigation file under the Data Act or VFOIA.

The court held that Keil was not entitled to access the information in the investigation file under the Data Act, Code § 2.2-3806(A), because he was not a "data subject" and also found that O'Sullivan's failure to respond to the March 9 letter was not a waiver of his defenses under the Data Act because the March 9, 2023 letter merely renewed the prior request for information. The court dismissed the action, and this appeal followed.

[2] The brief was apparently filed on July 12, but it does not appear in the record. The record does include O'Sullivan's opposition brief to Keil's complaint and motion for judgment, which was filed on July 7, and that memorandum does discuss the incident with relative detail.

ANALYSIS

This case requires us to interpret two statutes, the Data Act and VFOIA, and we do this de novo. *Hawkins v. Town of South Hill*, 301 Va. 416, 424 (2022). When applying either of these laws "turns on the specific facts of the case, we owe deference to the trial court's factual findings." *Suffolk City Sch. Bd. v. Wahlstrom*, 302 Va. 188, 205 (2023). Such findings will not be disturbed on appeal unless "they are 'plainly wrong or without evidence to support them.'" *Id.* (quoting *Grayson v. Westwood Bldgs. L.P.*, 300 Va. 25, 58 (2021)). In interpreting both statutes, "our task 'is to ascertain and give effect to legislative intent, as expressed by the language used in the statute.'" *Verizon Va. LLC v. State Corp. Comm'n*, 302 Va. 467, 477 (2023) (quoting *Cuccinelli v. Rector & Visitors of the Univ. of Va.*, 283 Va. 420, 425 (2012)). "[C]ourts apply the plain meaning . . . unless the terms are ambiguous or applying the plain language would lead to an absurd result." *Taylor v. Commonwealth*, 298 Va. 336, 341 (2020) (second alteration in original) (quoting *Baker v. Commonwealth*, 284 Va. 572, 576 (2012)).

I. Keil is not a "data subject," so the trial court did not err in concluding he was not entitled to receive a copy of the investigation file under the Data Act.

Keil raises several overlapping assignments of error, many of which turn on whether he is a "data subject" for the purposes of inspecting the internal investigation file under Code § 2.2-3806(A)(3). Before interpreting the statute, and specifically the phrase "data subject," we frame our discussion by looking to the General Assembly's intent and purpose in enacting the Data Act. *Hawkins*, 301 Va. at 425 ("Our function is to interpret the statute in a manner that reflects the legislative intent.").

A. The purpose of the Data Act

The General Assembly passed the first iteration of the Data Act in 1976 to address "concerns over potentially abusive information-gathering practices by the government, including

enhanced availability of such personal information through technology." *Carraway v. Hill*, 265 Va. 20, 23 (2003).[3]

The purpose of the Data Act is "to provide standards which a government agency must follow in the operation of personal information systems." *Id.* In establishing the Data Act, the General Assembly found that "legislation . . . to establish procedures to govern information systems containing records on individuals" was "necessary" "to preserve the rights guaranteed a citizen in a free society." Code § 2.2-3800(B)(4). The General Assembly's other findings included that: "[a]n individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information," "[t]he increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices," and "[a]n individual's opportunities to secure employment, insurance, credit, and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems." Code § 2.2-3800(B)(1)-(3). In sum, the Data Act seeks to protect personal information from misuse by government agencies.

B. The rights provided in Code § 2.2-3806 extend only to "data subjects."

Along with providing general protection from the misuse of personal information, the Data Act also provides specific rights to certain individuals who qualify as "data subjects" under the statute, including the right to inspect the subject's personal information. Code § 2.2-3806(A)(3). A data subject may also "challenge, correct, or explain information about him in the information system." Code § 2.2-3806(A)(5). The Data Act, therefore, ensures that those

[3] At that time, the Data Act was called "the Privacy Protection Act of 1976." *Carraway*, 265 Va. at 23 n.*. It was "repealed and reenacted under its current name [the Government Data Dissemination Act] without substantive change, effective October 1, 2001." *Id. See also Hinderliter v. Humphries*, 224 Va. 439, 442-44 (1982) (discussing the legislative history of the Data Act).

individuals have enumerated and specific rights to check the power of the agency collecting their information.

Turning to the statute's text, "[a]ny agency maintaining personal information shall . . . [u]pon request and proper identification of any data subject, or of his authorized agent, grant the data subject or agent the right to inspect, in a form comprehensible to him . . . [a]ll personal information about that data subject," subject to exclusions not relevant here. Code § 2.2-3806(A), (A)(3), (A)(3)(a).

Relevant terms are each defined in Code § 2.2-3801:

> "Data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system.
>
> "Personal information" means all information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.
>
> "Information system" means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

The trial court concluded that Keil is not the "data subject" of the internal affairs investigation file because the evidence at trial showed that the file is not indexed or searchable

by an "employee's name, personal number or other identifiable particulars." Instead, the file was organized by year, with each investigation assigned a sequential number. Keil argues that he qualifies because he is "an individual *about whom* personal information is indexed or may be located under identifiable particulars." He suggests "identifiable particulars" include his involvement in the internal affairs investigation, which led to the creation of the file in the first place. Keil stresses that the internal investigation file must contain "'identifying information' about Keil" because O'Sullivan and investigators were "in fact" able to locate the file. Summed up, Keil argues that "if there were no 'identifiable particulars' relating to Keil it would have been and would remain difficult or impossible for O'Sullivan and his subordinates to find and review the particular Internal Affairs file at issue."

C. Someone is only a "data subject" if information is organized or stored based on the person's name, personal number, or other "identifiable particulars."

To begin with, we agree with the parties that whether someone is a "data subject" depends on the way his personal information is stored and able to be retrieved. Again, a "data subject" is someone "about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system." Code § 2.2-3801. The natural reading of this phrase is that "under his name, personal number, or other identifiable particulars" modifies both "indexed" and "may be located." Personal information cannot be "indexed" by these features unless it is arranged or stored by those features. Nor can personal information be located *under* a name or number unless it is organized by that name or number.

Thus, we affirm that for a data subject's personal information to be "indexed" or "located" under his name, personal number, or other "identifiable particulars," his name,

number, or other "identifiable particulars" must be the key that leads the researcher to the place where the record may be found.[4]

D. "Identifiable particulars" are unique identifying details about the person who is the subject of the data.

The key question is what qualifies as an "identifiable particular[]." In interpreting a statutory phrase, we must infer the legislature's intent from the plain meaning of the language, assigning an undefined term its "ordinary meaning, given the context in which it is used." *Taylor v. Commonwealth*, 298 Va. 336, 342 (2020) (quoting *Lawlor v. Commonwealth*, 285 Va. 187, 237 (2013)). The "plain, obvious, and rational meaning" is "preferred over any curious, narrow, or strained construction." *Id.* (quoting *Lawlor*, 285 Va. at 237).

Revisiting the relevant statutory definition, to be a data subject, one's personal information must be indexed or located under one of the following types of information: "name, personal number, or other identifiable particulars." Code § 2.2-3801. Both a "name" and "personal number" are specific identifiers unique to an individual. The phrase "identifiable particulars" should be similarly understood as not just any piece of information, but a unique identifying characteristic of the person. This result yields the only interpretation that gives effect to the word "other," which precedes the phrase "identifiable particulars." That "other identifiable particulars" follows the delineated details of name and personal number

[4] In *Hinderliter*, 224 Va. at 445, the Supreme Court concluded that a police officer with personal information in an internal investigation file was a data subject, without discussing in any detail why the officer so qualified. However, we note that there, the report at issue was placed in the officer's "personnel file" and that "there [were] separate files on each officer, lodged in the Chief's office, arranged alphabetically by the individual's name." *Id.* While the Court did not parse the definition of "data subject" in depth or engage with the facts that illustrated how the file was located and retrieved, it is clear that the file holding the investigation report was organized alphabetically by name, and thus plainly "indexed" by name, falling squarely within the definition of "data subject." We also note that a circuit court decision cited by Keil, *McChrystal v. Fairfax County Board of Supervisors*, 67 Va. Cir. 171 (2005), did not include any examination of whether the plaintiff was a data subject or otherwise analyze that term.

demonstrates that the General Assembly intended for the "identifiable particulars" to be an additional, similar, identifying detail.

This conclusion is also supported by the *noscitur a sociis* canon of statutory interpretation, which "requires that 'words grouped in a list should be given related meaning.'" *Sainani v. Belmont Glen Homeowners Ass'n*, 297 Va. 714, 725 (2019) (quoting *Third Nat'l Bank in Nashville v. Impac Ltd.*, 432 U.S. 312, 322 (1977)). "[W]hen general and specific words are grouped, the general words are limited by the specific and will be construed to embrace only objects similar in nature to those things identified by the specific words." *Tomlin v. Commonwealth*, 302 Va. 356, 369 (2023) (emphases omitted) (quoting *Sainani*, 297 Va. at 724). Limiting the general word "identifiable particulars" by the more specific terms that precede it, an identifiable particular is not just any piece of information, but a unique identifying characteristic.

This is the same reasoning the Supreme Court applied in interpreting the nearly identical phrase appearing in the Data Act's definition of "information system," and it leads us to the same result. *Neal v. Fairfax Cnty. Police Dep't (Neal I)*, 295 Va. 334, 347-48 (2018). In *Neal I*, the Court considered whether automated license plate readers (ALPRs) constituted an "information system." As discussed above, a "data subject" is an "individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system." Code § 2.2-3801. And an "information system" "means the total components and operations of a record-keeping process . . . containing personal information and the name, personal number, or other *identifying particulars* of a data subject." *Id.* (emphasis added). Noting that "identifying particulars" is undefined, the Court applied the canon of *noscitur a sociis* and reasoned that "identifying particulars" must "include 'matters of the same import' as the more specific terms listed." *Neal I*, 295 Va. at 347-48. Accordingly, a license plate number could be an "identifying particular" because "it has the potential to identify

the individual to whom the plate number is registered in the same way a 'name' or 'personal number' identifies the individual to which it is assigned." *Id.* at 348.[5]

The *Neal I* Court's construction of "identifying particulars" in the definition of "information system" underscores the validity of our construction of the term "identifiable particulars" in the definition of "data subject." While the terms differ slightly, they are best understood as interchangeable because they appear in the same phrases ("name, personal number, or other identifiable particulars" and "name, personal number, or other identifying particulars"). Like the *Neal I* Court, we construe "identifiable particulars" to refer to a specific and unique item of information that categorically identifies the subject of the personal information maintained by the agency.

Keil's argument for an expansive interpretation of "identifiable particulars," unmoored from any details about a particular person, is further undermined by the interaction of the definitions of "information system" and "data subject." An information system is the record-keeping process that has both personal information about a data subject, and the "name, personal number, or other identifying particulars" about that data subject. Keil's argument is essentially that a data subject is anyone with personal information in an information system. But this ignores the actual definition of "data subject," which requires something more—that the personal

[5] Ultimately, the Court concluded that the record was insufficient to determine whether the components of the ALPR record-keeping process provide for a way to link a license plate to the vehicle owner. *Neal I*, 295 Va. at 348. But, after remand, the Court found that the ALPR record-keeping process did not "provide a means through which a link between a license plate number and a vehicle's owner" could be established. *Neal v. Fairfax Cnty. Police Dep't (Neal II)*, 299 Va. 253, 269 (2020). "The ALPR database does not contain 'the name, personal number, or other identifying particulars of an individual,'" pursuant to the definition of an information system because the ALPR does not "allow the Police Department to learn 'the name, personal number, or other identifying particulars of a data subject.'" *Id.* As a result, the Court found that "the Police Department's passive use of the ALPR system is lawful under the Data Act." *Id.*

information be organized by "name, personal number, or other identifiable particulars." Code § 2.2-3801.

Finally, we observe that relevant dictionary definitions lead to the same result we reach. "Particulars" are "the specific facts about a person's background," *Particulars*, *Black's Law Dictionary* (12th ed. 2024), or, more generally, "a specific item of information," *Particular*, *Webster's Third New International Dictionary* (2002). The phrase "identifiable particulars" literally refers to specific items of information that are "capable of being identified." *Identifiable*, *Webster's Third International Dictionary*, *supra*. But viewed in the context of the surrounding words, an "identifiable particular" is an item of information "capable of" identifying *the subject of the data*, and not simply a datum "capable of being identified" without reference to the data subject.

Our interpretation of the Data Act also aligns with the interpretation federal courts have applied to the Data Act's "federal counterpart," the Federal Privacy Act of 1974. *Hinderliter v. Humphries*, 224 Va. 439, 443 n.* (1982). Like the Data Act, Congress passed the Federal Privacy Act in response to "obvious threats the computer poses to privacy" and the "increasing growth of information-gathering by Government and private organizations," which did not have standards to regulate them.[6] And the Federal Privacy Act similarly gives individuals the right to request from agencies certain "records" contained in a "system of records." 5 U.S.C. § 552a. The "records" must include some item of information that identifies the individual seeking the information, and the "system of records" must be organized so that the information is "retriev[able]" by an "identifying number" or "symbol," or "other identifying particular assigned

[6] Joint Comm. on Gov't Operations, 94th Cong., Legislative History of the Privacy Act of 1974, at 6 (1976), https://www.justice.gov/d9/privacy_source_book.pdf [https://perma.cc/86TU-L94C].

to the individual."[7] 5 U.S.C. § 552a(4). Many federal courts have concluded that to enforce the Privacy Act, it is not enough that an agency has a record with identifying information about an individual; that record must exist within a "system of records" indexed according to unique personal characteristics.[8]

E. Keil is not a "data subject" entitled to receive the internal investigation file.

Applying our interpretation of "data subject" to Keil, the trial court was correct to conclude that Keil was not a "data subject" entitled to request information under the Act. The investigation file certainly contains "personal information" about Keil, but the file is not indexed or located by reference to Keil's name or other "identifiable particulars." Instead, the trial court made the factual finding that the investigation file was indexed by year and assigned a sequential number. There is no evidence that the number assigned to his file was assigned according to any

[7] Keil argues that the Data Act provides broader rights than the Federal Privacy Act because it uses the phrase "may be located under" instead of "retrievable." But there is no meaningful difference between the two phrases—"to retrieve" means "to find" or "to discover again," *Retrieve, Webster's Third International Dictionary, supra*, and is functionally the same as "to locate," which is "to determine or indicate the place of," or "to seek out and discover the position of" *Locate, Webster's Third International Dictionary, supra*. Keil also suggests there is a meaningful difference because the "system of records" defined in the Federal Privacy Act must be organized by number, symbol, or "other identifying particular *assigned to the individual*," whereas the Data Act lacks this language. But, as discussed above, the context of the phrase "identifiable particular" plainly refers to particulars "assigned to the individual."

[8] The Fifth Circuit has explained that "[t]he threshold issue in any claim alleging denial of access under the Privacy Act is whether the records sought by the plaintiff are maintained in a 'system of records' retrievable by an 'identifying particular assigned to' the plaintiff," and collected cases concluding the same. *Bettersworth v. FDIC*, 248 F.3d 386, 391 (5th Cir. 2001); *see also Paige v. Drug Enf't Admin.*, 665 F.3d 1355, 1360 (D.C. Cir. 2012) (Record video was "unmarked and bore no notation indicating its contents," and a "file number for documents and items related to" the subject of the video contained no "name or other personal identifier," and was therefore not subject to the Privacy Act.); *Kitlinski v. Barr*, No. 1:16-cv-0060, 2019 U.S. Dist. LEXIS 226313, at *24 (E.D. Va. Apr. 10, 2019) (Because the records "were archived only in a file system retrievable by the vacancy number of the announcement, and not by [plaintiff's] name, they fall outside of the scope of the Act.").

personal characteristic of Keil or was linked to any other unique identifier. Thus, Keil was not a data subject.

Only an individual who fits the definition of a "data subject" has a right to inspect personal information maintained by a government agency. Code § 2.2-3806(A)(3). Because Keil was not a "data subject," he is not entitled to relief for being refused the right to inspect records containing his personal information under Code § 2.2-3806.

II. O'Sullivan's failure to separately respond to Keil's March 9 and March 28, 2023 VFOIA requests did not entitle Keil to relief.

Next, we turn to Keil's contention that he is entitled to relief because O'Sullivan failed to separately respond to his information requests under VFOIA. In enacting VFOIA, the General Assembly intended to "ensure[] the people of the Commonwealth ready access to public records in the custody of a public body or its officers and employees, and free entry to meetings of public bodies wherein the business of the people is being conducted." Code § 2.2-3700(B). In this way, "[i]ts primary purpose is to facilitate openness in the administration of government," *Am. Tradition Inst. v. Rector & Visitors of the Univ. of Va.*, 287 Va. 330, 339 (2014), in order to "allow[] [for] an informed citizenry," *Gloss v. Wheeler*, 302 Va. 258, 288 (2023). VFOIA sets out specific procedures for responding to requests made under the Act. After an individual makes a request for public records "identify[ing] the requested records with reasonable specificity," the public body to which the request is sent "shall promptly, but in all cases within five working days of receiving a request, provide the requested records to the requester." Code § 2.2-3704(B). Alternatively, the public body may respond that the requested records are being partially or entirely withheld, that the records do not exist or cannot be found, or that it is impossible to provide the records within the five-day period. *Id*.

Two provisions of VFOIA address a failure to respond to a request for records. Under Code § 2.2-3704(E), the "[f]ailure to respond to a request for records shall be deemed a denial of

the request and shall constitute a violation" of VFOIA. Additionally, "[a]ny failure by a public body to follow the procedures established by this chapter shall be presumed to be a violation of this chapter." Code § 2.2-3713(E); *see, e.g.*, *Fenter v. Norfolk Airport Auth.*, 274 Va. 524, 532-33 (2007) (finding that the agency's "failure to properly respond to [a citizen's] second and third requests for information constituted a violation of [VFOIA]" and that the citizen was "entitled to recover reasonable costs and attorney's fees").

Keil sought two categories of information. First, on January 6, 2023, he requested information related to the investigation into the incident at the Chesapeake jail, invoking the federal FOIA statute. O'Sullivan responded on January 13 that he was considering the original letter to be a request under VFOIA and that he was exempt from providing the requested information under Code § 2.2-3706(B)(9) and (B)(4). On January 20, Keil clarified that he was requesting the same information under VFOIA, and three days later O'Sullivan replied again claiming the same exemptions to disclosure. The second category of information Keil sought was personnel information. He first requested his personnel file under VFOIA on February 9. The next day, O'Sullivan's counsel responded and informed Keil that his personnel file would be made available to him shortly.

Then, on March 9, Keil "renewed" his request for the information sought in "the original FOIA request dated January 6, 2023." This letter also stated that "the information requested in the January 6, 2023 letter and the follow-up communications . . . should include a copy of the entire employment/personnel file that Sheriff O'Sullivan and/or his office maintains on Matt Keil, including all sub-files and records covered by [the Data Act]." The letter added, "To be clear, Matt Keil has requested and continues to request a copy of all of the evidence, records, video, and information (both tangible and electronic) that relates in any manner to and/or supports the demotion decision that was announced to Matt Keil" in December 2022. Finally,

the letter sought "any additional responsive information that relates in any manner to Matt Keil's appeal of that decision and/or the denial of his appeal." O'Sullivan did not respond to this request.

The trial court found that "based upon the plain title of the letter," the March 9 letter was "a renewed request and seeks clarification of the response to the original request" that was sent on January 6 and that O'Sullivan properly claimed the exemption in Code § 2.2-3706(B)(9) in his response to that first letter and request. Thus, O'Sullivan's failure to respond to the March 9 request did not violate VFOIA. Keil argues this conclusion was in error because the March 9 letter was a new or supplemental request seeking "new records and information," including "anything else that may have been created after the date of the prior requests."

We find that the record supports the trial court's assessment. By its own terms, the March 9 letter sought the same category of information that Keil already "ha[d] requested." And O'Sullivan had already responded to requests for the same two broad categories of information sought in the March 9 letter—information relating to the internal affairs investigation and Keil's entire employment/personnel file. We therefore find that the trial court was correct that the letter sought the same information relating to the internal affairs investigation and personnel information that was previously requested and to which O'Sullivan had previously responded.[9]

III. O'Sullivan's failure to respond to Keil's Data Act request did not waive his right to claim defenses under the Act.

Keil also argues that O'Sullivan's responses never referenced the Data Act, or complied with the procedures of the Data Act. This failure to respond, Keil argues, should mean

[9] Even if O'Sullivan violated VFOIA by not separately responding to the March 9 letter, it is not evident that Keil would be entitled to any relief. While a failure to respond to a VFOIA request is a violation of the Act, the petitioner is only "entitled to recover reasonable costs . . . and attorney fees from the public body if the petitioner substantially prevails on the merits of the case." Code § 2.2-3713(D). Keil has not argued that he substantially prevailed on the merits of the case.

O'Sullivan waived any ability to argue that Keil did not qualify to receive information under the Data Act. In essence, Keil asserts that anyone who cites the Data Act and does not receive a timely response should be automatically entitled to whatever they requested, whether it fits within the Data Act or not.

The Data Act incorporates VFOIA's response procedures, including the requirement that a denial of a request "shall identify with reasonable particularity . . . the specific Code section that authorizes the withholding of the records." Code § 2.2-3704(B)(1); *see* Code § 2.2-3806(A)(4)(a) (incorporating "the procedures set forth in subsections B and C of Code § 2.2-3704 for responding to requests under [VFOIA]"). The natural reading of this section is that an agency must cite the specific sections of the *Data Act* that entitles the agency to withhold the record. The Data Act contains different exemptions than VFOIA, *see* Code § 2.2-3802, and none correspond with O'Sullivan's claimed exemptions under VFOIA.[10] An agency must separately respond to a request under the Data Act, and we agree with Keil that O'Sullivan failed to do so.

But this failure does not result in the waiver Keil seeks. While the Data Act incorporates VFOIA's response procedures, it has its own remedy provision for a failure to respond: "[a]ny aggrieved person may institute a proceeding for injunction or mandamus against any person or agency that has engaged, is engaged, or is about to engage in any acts or practices in violation of

[10] Below, O'Sullivan claimed that both Code § 2.2-3706(B)(9) and (B)(4) of VFOIA exempt the internal investigation materials from mandatory disclosure. The latter section exempts "records of persons imprisoned in penal institutions in the Commonwealth, provided such records related to the imprisonment." The closest exclusion in the Data Act is § 2.2-3802(7)(d), which states that "[t]he provisions of this chapter shall not apply to personal information systems: . . . (7) Maintained by any of the following and that deal with investigations and intelligence gathering related to criminal activity: . . . d. Sheriff's departments of counties and cities." On appeal, O'Sullivan only emphasizes his exemption under § 2.2-3706(B)(9), which exempts from mandatory disclosure "[r]ecords of . . . (ii) administrative investigations relating to allegations of wrongdoing by employees of a law enforcement agency." No exemption exists under the Data Act for administrative investigation materials.

the provisions of this chapter." Code § 2.2-3809. Thus, a violation of the procedures required by the Data Act, including failing to comply with the disclosure procedures, *may* entitle an "aggrieved person" to injunctive or mandamus relief.

But Keil is not a data subject, so he is not entitled to injunctive or mandamus relief. First, as we have shown, Keil is not the "subject" of the investigation file because it was not indexed or located by reference to any of his "identifiable particulars." Keil also requested access to "all personnel file[s]" pursuant to the Data Act, but he presented no evidence about the method of storing the personnel files from which it could be concluded he qualifies as a "data subject."

The Supreme Court's decision in *Lawrence v. Jenkins*, 258 Va. 598, 603 (1999), which concerned a zoning administrator's failure to properly cite an exemption in a VFOIA case, also shows that Keil is not entitled to relief. There, the administrator's response did not comply with the exact requirements of VFOIA. Even so, the Supreme Court concluded it was error for the trial court to issue a writ of mandamus to compel the administrator to comply with VFOIA "solely because the zoning administrator, in electing to exercise an exemption provided in FOIA, failed to timely refer to the specific Code section making that portion of the requested documents exempt." *Id.* at 602. Because one of the elements of a writ of mandamus is "the clear right of the petitioner to the relief being sought," and the information sought was subject to the claimed exemption, the plaintiff did not have a clear right to access the information. *Id.* at 603. Thus, the administrator's failure to cite the code provision "did not operate as a waiver of Lawrence's otherwise valid exercise of an applicable exemption." *Id.*

While the error here was of a different type, and under a different Act, the rules of mandamus are the same. Keil has not established that he is a data subject, and so has not established that he has a "clear right" to the relief he seeks—access to the investigation file and personnel file under the Data Act. Even assuming Keil is the data subject of his personnel file,

Keil is not entitled to mandamus or injunctive relief because he received his personnel file shortly after requesting access to it. For this reason, O'Sullivan's failure to respond to Keil's requests for information under the Data Act does not entitle Keil to any relief.

IV. Keil failed to show that O'Sullivan unlawfully disseminated his personal information under Code § 2.2-3803(A)(1).

Next, Keil argues that the trial court erred in failing to find that O'Sullivan violated the Data Act when O'Sullivan "unlawfully and unnecessarily disseminated information about Keil" that was contained in the internal affairs investigation file during the litigation. Keil particularly focuses on an exchange that occurred during his cross-examination at trial where O'Sullivan's counsel asked Keil about the "investigation [into] what happened the night you were supervising the inmate . . . and his jaw was broken?" In addition, Keil points to one of O'Sullivan's pre-trial briefs which described the use of force that resulted in the internal affairs investigation into Keil. Keil argues that these disclosures violate Code § 2.2-3803(A)(1), which requires "[a]ny agency maintaining an information system that includes personal information" to "[c]ollect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency."

The trial court rejected Keil's claim for the unlawful dissemination of personal information because he is not a "data subject." But unlike the other sections of the Data Act that Keil tried to enforce to obtain the information in the investigation file, Code § 2.2-3803(A)(1) does not limit its protection against dissemination of information to individuals who qualify as "data subjects." Instead, a violation of this section may be remedied by the mechanisms in Code § 2.2-3809, discussed above. Anyone whose personal information is disseminated in violation of this section may be an "aggrieved person" who "may institute a proceeding for injunction or mandamus" against the individual or agency who is engaging in a violation of this section. Code

§ 2.2-3809. Then, if the "aggrieved party" is "successful," "the agency enjoined or made subject to a writ of mandamus by the court shall be liable for the costs of the action together with reasonable attorneys' fees as determined by the court." *Id.*

We find that Keil is an aggrieved party because he alleges that a government agency violated the Act by disseminating his personal information contrary to the procedures prescribed in the Act. *See* Code § 2.2-3801 ("Personal information means all information that . . . describes . . . anything about an individual, including . . . [his] criminal or employment record."). While we disagree with the trial court's determination that the Data Act does not apply to Keil at all because Keil is not a data subject, we conclude that the trial court was ultimately right that Keil is not entitled to relief under this portion of the Data Act.[11]

To enforce a claim under Code § 2.2-3803(A)(1), "the burden [is] on the plaintiff to establish a lack of necessity or an improper purpose for the dissemination." *Hinderliter*, 224 Va. at 448 (considering a violation under the Data Act's predecessor statute). "There is a presumption that public officials will obey the law. And there is nothing in the [Data Act] that reverses such presumption or imposes the ultimate burden of proof on defendants sued under the Act." *Id.* (citation omitted). Thus, "the presumption stands until rebutted by contrary evidence." *Id.* Finally, whether the dissemination of the information was proper "must be viewed from the perspective of the 'agency' charged with violation of the Act." *Id.*

The *Hinderliter* case exemplifies how the disclosure of the same information may be proper in some cases but improper in others. There, when a member of the County Board of

[11] "In instances where a trial court's decision is correct, but its reasoning is incorrect, and the record supports the correct reason, we uphold the judgment pursuant to the right result for the wrong reason doctrine." *Miller & Rhoads Bldg., L.L.C. v. City of Richmond*, 292 Va. 537, 542 (2016) (quoting *Haynes v. Haggerty*, 291 Va. 301, 305 (2016)). Here, the record supports our conclusion that Keil failed to meet his burden of "establish[ing] a lack of necessity or an improper purpose for the dissemination" of his information. *Hinderliter*, 224 Va. at 448.

Supervisors disseminated a report transcribing an investigation into police misconduct it was "unnecessary to accomplish any proper purpose of the Board of Supervisors" because she made the disclosure during her daughter's trial for misconduct, and so any dissemination "serve[d] the private interests of [her] and her daughter." *Id.* at 449-50. But the same plaintiff failed to show that the police chief's dissemination of the same report to the county executive was unnecessary or improper because the county executive was the "boss" of the chief, and was "vested with supervision and control of the police force." *Id.* at 449. Likewise, the plaintiff failed to show that the dissemination of the report from the county executive to the Board of Supervisors was improper because the Board of Supervisors was a "policy-determining body" concerned with "allegations of police brutality." *Id.* For these latter two disseminations, the "plaintiff did not establish a lack of necessity or an improper purpose." *Id.*

We conclude that Keil has failed to meet his burden to "establish a lack of necessity or an improper purpose for the dissemination." *Id.* at 447-48. Keil presented no evidence that O'Sullivan disseminated the report for an improper reason, or that the dissemination was not necessary and appropriate given the context of the sheriff's office defending itself in litigation that Keil initiated. To the contrary, Keil argues that "O'Sullivan never identified any requirement, need or proper purpose for the dissemination in which he and his lawyer engaged" and that "none of the purported facts were necessary or appropriate for purposes of any defense O'Sullivan asserted." But this improperly attempts to transfer the burden of defense onto the government actor, which *Hinderliter* prohibits. Because Keil failed to meet his burden under Code § 2.2-3803(A)(1), we find that Keil failed to show that O'Sullivan violated this section of the Data Act.

V. Keil failed to show that the late disclosure of a missing part of his personnel file entitled him to relief under VFOIA or the Data Act.

Finally, Keil argues that he is entitled to relief based on the late disclosure of certain employment evaluations from his personnel file. After Keil requested a copy of his "entire employment/personnel [sic] that the Sheriff and/or his office maintains on [him], including all sub-files and records covered by [the Data Act]," on February 9, O'Sullivan provided it to him within days. Then, during trial in the general district court, when Keil asserted that employment evaluations from 2011 to 2018 did not appear in the file, O'Sullivan did not object to disclosing the evaluations. Instead, O'Sullivan noted that any exclusion was an "oversight," and he provided the missing evaluations 13 days later.

Keil has failed to show that O'Sullivan's late provision of the employment evaluations entitles him to relief under VFOIA. First, the record does not show that Keil petitioned for mandamus or injunction supported by an affidavit showing good cause, as required by Code § 2.2-3713(A). Moreover, by the time the trial court decided the case, there was no need to grant mandamus or injunctive relief under VFOIA because the evaluations had been provided to Keil. Finally, a petitioner is only "entitled to recover reasonable costs . . . and attorney fees from the public body if the petitioner substantially prevails on the merits of the case." Code § 2.2-3713(D). Keil has not argued on brief or below that he substantially prevailed on the merits of the case, nor could he show the same.

Neither does O'Sullivan's late provision of the evaluations entitle Keil to relief under the Data Act. Keil is only entitled to inspect information covered by the Data Act if he is a "data subject," Code § 2.2-3806(A)(3), but Keil presented no evidence about the method of storing the personnel files or employment evaluations from which it could be concluded he qualifies as a "data subject." Code § 2.2-3801. And, again, even if we assume that Keil is a data subject, we

would still find that Keil is not entitled to mandamus or injunctive relief because he received the evaluations.

While the trial court did not specifically address the late provision of this information in its order, we find that the court did not err in its ultimate conclusions that Keil was not entitled to any relief under either VFOIA or the Data Act.

CONCLUSION

For these reasons, we affirm.

Affirmed.